B. Setyo Ryanto

Optical Storage, Data pada Kepingan

Bagian 1 dari 2 Artikel

Optical drive sudah demikian populer penggunaannya pada PC. Bahkan hampir bisa dikatakan sebagai komponen wajib pada setiap PC, layaknya FDD pada satu dasawarsa yang silam.

Optical storage bukan lagi sesuatu yang baru penggunaannya pada dunia PC. Namun, pengembangannya tiada henti. Utamanya pada pengembangan kapasitas penyimpanannya.

Pada kesempatan kali ini, pembahasan akan lebih difokuskan pada tren dan pengembangannya dalam waktu dekat. Tentunya Anda sudah lebih lama dan mengenal lebih dekat dengan CD. Optical storage yang satu ini memang sangat populer, terlebih dengan harganya yang sangat terjangkau. Juga untuk masalah kompatibilitas, yang agaknya mulai menjadi masalah pada penerusnya—DVD (akronim untuk *Digital Versatile Disc* ataupun *Digital Video Disc*)—yang akan dijelaskan pada penjelasan selanjutnya.

FIRST-GENERATION OPTICAL DISCS
Compact Disc (CD)
Laserdisc
Magneto-optical disc
Ultra Density Optical
SECOND-GENERATION OPTICAL DISCS
Minidisc
Digital Versatile Disc (DVD)
Digital Multilayer Disk
Digital Video Express
Fluorescent Multilayer Disc
GD-ROM
Phase-change Dual
Universal Media Disc
THIRD-GENERATION OPTICAL DISCS
Blu-Ray Disc
Enhanced Versatile Disc
Forward Versatile Disc
Holographic Versatile Disc
HD DVD
Professional Disc for DATA
Versatile Multilayer Disc

Optical storage, dari generasi ke generasi.

Namun, pembahasan kali ini akan lebih difokuskan mulai dari era DVD, berikut pengembangannya lebih lanjut. Dilengkapi juga dengan FAQ, yang merupakan pertanyaan yang sering terlontar pada saat membicarakan optical storage.

Perkembangan Optical Storage

DVD diperkenalkan pada tahun 1996, awalnya sebagai Digital Video Disc. Namun, pengembangan penggunaanya lebih lanjut membuatnya lebih dikenal sebagai Digital Versatile Disc. Secara fisik memiliki banyak kesamaan dengan CD, namun perbedaan kapasitasnya cukup signifikan. Sangat wajar, mengingat DVD adalah generasi kedua dari teknologi optical storage.

CD bersama dengan laserdisc adalah generasi pertama. Penggunaannya lebih banyak untuk music dan *software*/data. Keterbatasan penyimpanan data pada generasi ini membuatnya kurang ideal untuk video. Dibutuhkan permukaan yang lebar seperti laserdisc untuk optimal.

Generasi kedua mulai berkembang tahun 1990-an. Mampu menyimpan data dengan kapasitas lebih besar. Sehingga dipandang ideal untuk kebutuhan video sekarang. Generasi inilah yang sedang populer saat ini.

Generasi ketiga sebagian masih dalam taraf pengembangan. Ditujukan untuk mampu menyimpan *high-definition* video. Kapasitasnya yang bertambah juga memungkinkan menyimpan data jauh lebih besar, juga pemanfaatan pada video games *console* dengan detail gambar yang mendekati dunia nyata.

DVD Technical Information

Seperti juga CD, DVD terdiri dari dua jenis lapisan utama. Lapisan pertama dari bahan *polycarbonate plastic*, lapisan kedua bertugas sebagai *reflective layer* dari bahan alumunium atau emas. Kedua lapisan tersebut digabungkan, menjadi sebuah kepingan dengan ketebalan 1,2 mm. Data dapat diakses dari salah satu sisi (untuk *single-sided*) dan dari kedua sisi (pada *doube-sided disc*).

Jika CD menggunakan teknologi laser dengan panjang gelombang 780 nm dan *numerical aperture* pada 0,45, bandingan dengan DVD yang sudah menggunakan panjang gelombang 650 nm dengan numerical aperture pada 0,6. Dari perbe-

Tabel DVD Specification

FEATURES	DVD
ATTRIBUTES & PARAMETERS	**DIGITAL VERSATILE DISC**
Technology	Red Laser
Disc Diameter	120 mm
Disc Thickness	1.2 mm
Centre Hole	15 mm
Laser Wavelength	650 nm
Numerical Aperture	0.6 & 0.65
Track Pitch	0.74 µm
Shortest Pit	0.4/0.44 µm
Jitter	7-8 %
Maximum Data Layers/Side	2
Layer Capacity	4.7 GB
Maximum Capacity	8.5 GB / Side
Maximum Data Transfer Rate	11 Mbps
Content Protection	CCS, 40 bit
Encoding (DVD-Video)	MPEG-2
Video FPS	480, 576/24p, 50, 60i
Compatibility	CD

Tabel DVD Physical Format Standards

(ECMA INTERNATIONAL AND ISO/IEC)			
FORMAT	DESCRIPTION	ECMA STANDARD	ISO/IEC STANDARD
DVD-ROM	80 mm disc	268 (Apr. 01)	16449:2002 (Apr. 02)
DVD-ROM	120 mm disc	267 (Apr. 01)	16448:2002 (Apr. 02)
DVD-R (G)	120 mm & 80 mm disc (4.7 GB & 1.46 GB)	NA	NA
DVD-R (A)	120 mm & 80 mm disc (4.7 GB & 1.46 GB)	NA	NA
DVD-R	120 mm & 80 mm disc (3.95 GB & 1.23 GB)	279 (Dec. 98)	20563:2001 (July 01)
DVD+R	120 mm & 80 mm disc (4.7 GB & 1.46 GB)	349 (Dec. 03)	DIS 17344
DVD-RW	120 mm & 80 mm disc (4.7 GB & 1.46 GB)	338 (Dec. 02)	DIS 17342
DVD+RW	120 mm & 80 mm disc (4.7 GB & 1.46 GB)	337 (Dec. 03)	DIS 17341
DVD-RAM	120 mm & 80 mm disc case	331 (Dec. 01)	DIS 17594
DVD-RAM	120 mm & 80 mm disc (4.7 GB & 1.46 GB)	330 (June 02)	DIS 17592
DVD-RAM	120 mm disc case	273 (Feb. 98)	16825: 1999 (May 99)
DVD-RAM	120 mm disc (2.6 GB)	272 (June 99)	16824: 1999 (May 99)

Beragam format DVD yang telah beredar.

daan panjang gelombang dan numerical aperture, didapatkan peningkatan efisiensi *densisty* hingga 3,5 kali. Masih ditambah dengan penggunaan coding DVD yang lebih efisien. Seperti digantinya error correction CIRC (Cross Interleaved Reed-Solomon Code) yang digunakan pada CD dengan Reed-Solomon Product Code (RS-PC) pada DVD. Keterangan tambahan lain mengenai spesifikasi DVD dapat dilihat pada tabel.

Apa Itu DVD Format?

Seperti pada CD-Recordable (CD-R), DVD juga memiliki format untuk *write-once*, di mana penggunaan materi *dye recording* layer tidak memiliki kemampuan *reversible*. Namun berbeda dengan CD-R, pada teknologi DVD terdapat lima macam format untuk write-once: DVD-R, DVD+R, DVD-RW, DVD+RW, dan DVD-RAM.

DVD-RW dan DVD+RW lebih mirip dengan CD-ReWriteable (CD-RW), dengan menggunakan recording layer yang dapat diubah-ubah (phase-change recording layer) oleh writing laser pada DVD writer drive. Kemampuan tulis ulangnya kurang lebih sebanyak 1.000 kali.

Dengan teknologi serupa, DVD-RAM mampu ditulis ulang hingga 100.000 kali. Dilengkapi dengan *hard sector*, kemampuan *random access*, dan beberapa dilengkapi dengan sebuah *cartridge*. DVD-RAM lebih tepat jika dibandingkan layaknya sebuah harddisk pada PC, daripada dibandingkan dengan DVD-RW ataupun DVD+RW.

Saat diperkenalkan tahun 1997, DVD-R menggunakan teknologi laser dengan panjang gelombang 635 nm dan mampu menampung data sebesar 3,95 GB pada kepingan 12 cm. Ini dikenal sebagai DVD-R versi 1.0. Pada versi 1.9, kapasitasnya meningkat menjadi seperti yang kita ketahui sekarang 4,7 GB. Pembaruan tahun 2000, memisahkan antara DVD-R for Authoring dan DVD-R for General. DVD-R Authoring tetap menggunakan teknologi laser dengan panjang gelombang 635 nnm, dengan kapasitas terbatas pada 3,95 GB. Sedangkan, DVD-R for General menggunakan teknologi laser dengan panjang gelombang 650nm, sama seperti yang digunakan format DVD yang lain.

DVD-RW diperkenalkan pada tahun 1999 (versi 1.0), dengan kapasitas 4,7 GB pada kepingan berdiameter 12 cm. Namun masih memiliki masalah kompatibilitas. Baru pada tahun 2000 (versi 1.1) masalah ini diperbaiki.

DVD-RAM memulai debutnya pada tahun 1998. Versi 1.0 hanya memiliki kapasitas 2,6 GB pada keping 12 cm. Kapasitasnya berkembang menjadi 4,7 GB pada versi 2.0 di tahun 1999. Alternatif keping mini berdiameter 8 cm dengan kapasitas 1,46 GB (versi 2.1) diperkenalkan kemudian pada tahun 2000.

DVD+RW mulai dikenal di pasar luas pada tahun 2001. Dengan kapasitas 4,7GB untuk keping berdiameter 12 cm. Saat pengembangan sempat dikembangkan versi sebelumnya yang hanya memiliki kapasitas 3,0 GB. Selanjutnya, pada tahun 2002 mulai diperkenalkan DVD+R.

Kategori Standardisasi yang Digunakan untuk DVD

Jika pada era CD, dikenal standardisasi Yellow Book untuk CD-ROM (*Compact Disc-Read Only Memory*), Red Book untuk CD-DA (Compact Disc - Digital Audio), Orange Book untuk CD-R. Demikian juga pada format DVD.

Standardisasi ini mencakup karakteristik optical signal, susunan fisik, metoda *writing, file system,* dan seterusnya. Baik sesuai dengan format (DVD-ROM, DVD-R, DVD-RW, DVD-RAM), mapun penggunaannya yang spesifik (DVD-Video, DVD-Audio, DVD-ENAV, DVD-VR, DVD-AR, DVD-SR) standardisasinya diatur DVD Forum (dahulu dikenal dengan DVD Consortium). DVD Forum mulai terbentuk pada tahun 1995, yang terdiri dari gabungan manufaktur seperti Hitachi, Matsushita Electric, Mitsubishi Electric, Pioneer, Philips Electronics, Sony, Thomson, Time Warner, Toshiba, dan JVC.

Format DVD+R, DVD+RW dan DVD+MRW (Mount Rainier) diciptakan oleh DVD+RW Alliance. Dimulai pada tahun 1997, terdiri dari gabungan Philips Electronics, Hewlett-

DVD Data Transfer Rate

■ Seperti juga pada CD writer drive, kecepatannya di dalam satuan “x”. Faktor pengali kecepatan ini berlaku sama baik untuk proses *read, write,* maupun *rewrite*. Di mana untuk DVD, 1x = 1,32 MB/s (1.385.000 bytes/second). Jadi, jika kecepatan sebuah DVD writer untuk proses write adalah 4x, artinya ia mampu menuliskan data ke media DVD dengan kecepatan 5,28 MB/s.

Metoda saat proses write untuk media DVD juga masih sama dengan CD. Yaitu, *Constant Linear Velocity* (CLV), *Zoned Constant Linear Velocity* (ZCLV), dan *Constant Angular Velocity*.

Satuan x untuk kecepatan DVD dan CD sangat berbeda. 1x pada DVD setara dengan 9x pada CD. Untuk lebih jelasnya dapat melihat tabel.

Tabel DVD Data Transfer Rate

DVD READ/WRITE SPEED	TRANSFER RATE (BYTE/SEC)	TRANSFER RATE (KB/S)	TRANSFER RATE (MB/S)	EQUIVALENT CD TRANSFER RATE
1x	1,385,000	1,352.54	1.32	9x
2x	2,770,000	2,705.08	2.64	18x
3x	4,155,000	4,057.62	3.96	27x
4x	5,540,000	5,410.16	5.28	36x
5x	6,925,000	6,762.70	6.60	45x
6x	8,310,000	8,115.23	7.93	54x
8x	11,080,000	10,820.31	10.57	-
10x	13,850,000	13,525.39	13.21	-
12x	16,620,000	16,230.47	15.85	-
16x	22,160,000	21,640.63	21.13	-

Gigabyte vs Gibibyte

■ Sudah sejak lama ada perbedaan sudut pandang, dalam menentukan perhitungan dalam satuan byte. Seperti yang diketahui, perbedaan utama adalah pada perbedaan perhitungan berdasarkan bilangan biner (2^n) dan desimal (10^n).

Pada dunia komputer—di mana semuanya serba digital dan perhitungan berdasarkan bilangan biner—sering kali penggunaannya sedikit berbeda dengan penggunaan pada bilangan desimal, yang menjadi dasar pada SI (sistem internasional).

Seperti pada penulisan awalan satuan Giga, yang seharusnya menyatakan 10^9. Pada standardisasi IEC 60027-2, untuk telekomunikasi dan elektronik, ditambahkan sebuah kesepakatan baru dalam penyebutan. Khusus untuk dunia berbasis biner ini. Untuk satuan setara Gigabyte (GB = 10^9 byte), akan disebut sebagi Gibibyte (GiB = 2^30 byte = 1.073.741.824 byte). Lebih jelasnya dapat dilihat pada tabel.

Meskipun standar penamaan ini sudah mulai diterapkan pada tahun 1999, namun penggunaannya belum memasyarakat. Sehingga masih banyak sedikit kesalahpahaman untuk perbedaan yang satu ini.

Tabel Quantities of Bytes

POPULAR USE (INCLUDING LESSER USED SI DEFINITION)			ALTERNATIVE DEFINITIONS CREATED BY 1999 ADDENDUM TO (IEC 60027-2)		
NAME	SYMBOL	QUANTITY OF BYTES	NAME	SYMBOL	QUANTITY OF BYTES
kilobyte	KB	210 or 103	kibibyte	KiB	210
megabyte	MB	220 or 106	mebibyte	MiB	220
gigabyte	GB	230 or 109	gibibyte	GiB	230
terabyte	TB	240 or 1012	tebibyte	TiB	240
petabyte	PB	250 or 1015	pebibyte	PiB	250
exabyte	EB	260 or 1018	exbibyte	EiB	260
zettabyte	ZB	270 or 1021	zebibyte	ZiB	270
yottabyte	YB	280 or 1024	yobibyte	YiB	280

Packard, Mitsubishi Chemical, Ricoh, Sony, dan Yamaha.

Berbeda dengan CD yang menggunakan banyak "book" untuk setiap format. DVD menggunakan standar yang lebih sederhana. Data yang terdapat pada DVD seharusnya dapat terbaca baik dengan UDF filesystem maupun ISO9660 filesystem (UDF Bridge Format).

Apa Itu Universal Disc Format (UDF)?

Standardisasi untuk UDF kali pertama dikeluarkan oleh Optical Storage Technology Association (OSTA) pada tahun 1995. Sebuah file system untuk optical storage, tidak terbatas untuk DVD saja.

Seiring perkembangannya, UDF juga terus berkembang mengikuti zaman. Untuk DVD, versi UDF 1.02 adalah filesystem yang digunakan pada DVD-Video, DVD-Audio dan DVD-ROM. UDF 1.5 digunakan untuk incremental writing (*multisession*). Sedangkan UDF 2.0 adalah standar yang digunakan pada DVD-RW, DVD-RAM dan DVD Video Recording (DVD-VR) format.

Perangkat Apa Saja yang Dapat Melakukan Proses Write pada Media DVD?

Tidak hanya komponen PC, seperti pada DVD writer drive saja yang mampu melakukan hal ini. Beberapa perangkat elektronik lainnya pun sudah mampu melakukan hal ini. Seperti pada beberapa handycam, ataupun TiVo yang dilengkapi kemempuan write pada media DVD. Format yang digunakan beragam, namun kebanyakan menggunakan format berikut: DVD-R, DVD-RW, DVD+R, DVD+RW, dan DVD-RAM.

Berapa Kapasitas Sebenarnya dari Sebuah DVD?

Untuk media DVD dengan diameter 12 cm, akan memiliki kapasitas 4,7 GB untuk *single-sided* dan 9,4 untuk *double-sided*. Sedangkan dengan diameter 8 cm, akan memiliki kapasitas 1,46 GB single-sided dan 2,92 double-sided.

Namun, keterangan tersebut hanya berlaku untuk DVD dengan single layer. DVD memiliki penamaan khusus untuk hal ini. Penjelasan singkatnya antara lain adalah sebagai berikut:

- DVD-5: Single-sided/single-layer DVD dengan kapasitas penyimpanan 4,7 GB.
- DVD-9: Single-sided/dual-layer DVD dengan kapasitas penyimpanan 8,5 GB.
- DVD-10: Double-sided/single-layer DVD dengan kapasitas penyimpanan 9,4 GB.
- DVD-18: Double-sided/dual-layer DVD dengan kapasitas penyimpanan 17 GB.

Pengembangan media optical storage tentunya tidak berhenti sampai di sini. Berkembangnya kebutuhan, menyebabkannya terus mengembangkan, utamanya untuk urusan kapasitas. Berita tentang akan digunakannya penerus DVD, yaitu Blu-Ray pada game console PlayStation 3 tentunya sudah dinanti-nantikan. Belum lagi pengembangan HD-DVD. Apakah hanya itu saja? Penjelasan selanjutnya akan tersedia di edisi mendatang. ■

Tabel Writable DVD Disc Capacities

(UNFORMATTED SINGLE-SIDED, SINGLE-LAYER DISCS)				
DISC FORMAT	SPECIFICATION VERSION	DISC SIZE	NUMBER OF USER DATA SECTORS PER SIDE	GROSS CAPACITY (BYTES)
DVD+R	1.2	8 cm	714.54	1,463,386,112
		12 cm	2,295,104	4,700,372,992
DVD+RW	1.2	8 cm	714.54	1,463,386,112
		12 cm	2,295,104	4,700,372,992
DVD-R	1.0	8 cm	600.59	1,230,000,000
		12 cm	1,928,711	3,950,000,000
	Authoring 2.0	8 cm	712.89	1,460,000,000
		12 cm	2,294,922	4,700,000,000
	General 2.0	8 cm	712.89	1,460,000,000
		12 cm	2,294,922	4,700,000,000
DVD-RW	1.1	8 cm	712.89	1,460,000,000
		12 cm	2,294,922	4,700,000,000
DVD-RAM	1.0	12 cm	1,218,960	2,496,430,080
	2.0	12 cm	2,295,072	4,700,307,456
	2.1	8 cm	714.48	1,463,255,040

Lebih Lanjut

- **http://en.wikipedia.org/wiki/CD**
- **http://en.wikipedia.org/wiki/DVD-ROM**
- **http://en.wikipedia.org/wiki/Optical_disc**
- **http://www.osta.org/technology/dvdqa/**
- **http://www.mp3-cdburner.com/DVD-Glossary.shtml**
- **http://en.wikipedia.org/wiki/Gibibyte**

Hayri

Social Engineering: Ancam Keamanan Komputer

Senjata dan musuh yang paling berbahaya bagi manusia adalah manusia itu sendiri. Pernyataan ini tampaknya cukup mengena untuk menggambarkan bagaimana berbahayanya ancaman keamanan jaringan dan data yang bernama *Social Engineering*.

Halo selamat siang, dengan *customer support* ada yang bisa dibantu," seorang staf customer support menjawab telepon. "Halo saya mau tanya mengenai *account* internet suami saya, di mana ya alamat yang digunakan untuk mendaftar account tersebut," penelepon menjawab. "Bisa minta nomor customer-nya Bu," sang customer support membantu. "Oh saya juga lupa, tetapi saya tahu e-mail-nya, testing123@abcd.com. Cepat ya Mas saya agak terburu-buru nih sudah diminta sama suami saya," timpal sang penelepon. Tanpa rasa curiga sang customer support langsung memberikan alamat lengkap dari pelanggannya tersebut berikut dengan nomor teleponnya. Dan sesi peneleponan pun berakhir.

Pada minggu berikutnya datanglah seorang customer dengan beberapa pengacara ke kantor penyedia jasa tersebut. Ia melaporkan bahwa dirinya telah dicemarkan nama baiknya, telah dirusak rumah tangganya, dan telah difitnah oleh seorang wanita. Apa hubungannya wanita tersebut dengan penyedia jasa tadi? Ternyata wanita tersebut mendapatkan informasi alamat dan nomor telepon customer tadi dari sang customer support yang diteleponnya minggu kemarin.

Semua berasal dari alamat e-mail yang didapatnya dari halaman "friendster" milik customer tersebut. Rupanya saking kagumnya sang wanita kepada customer tadi, maka dicarilah alamat lengkapnya, dan sayangnya pihak penyedia jasalah yang memberikan informasi tersebut. Informasi yang seharusnya menjadi rahasia perusahaan dan privasi dari sang customer akhirnya dapat dengan mudah diberikan oleh staf customer support tadi kepada orang yang tidak berhak. Pada akhirnya, pihak penyedia jasa tersebut dituntut oleh sang customer dan memang terbukti kesalahan ada pada pihak penyedia jasa. Sampai di sini Anda sudah melihat salah satu contoh cerita fiksi dari pembobolan celah keamanan data dan informasi pribadi dengan menggunakan metode *Social Engineering*.

Bukan hanya kejadian yang terbilang cukup sepele ini saja yang merupakan contoh dari keberhasilan social engineering, data yang lebih penting pun banyak sekali yang bisa didapat dengan menggunakan teknik ini. Firewall secanggih apapun, setebal apapun lapisan keamanan Anda pada server atau perangkat jaringan, tidak akan bisa memblokir serangan yang satu ini. Karena musuh yang dihadapinya bukanlah virus, *script, trojan, backdoor, adware, spyware, keylogger,* dan lain sebagainya, melainkan adalah manusia itu sendiri.

Tekniknya pun sangat bervariasi dan bermacam-macam, tidak hanya melalui telepon saja. Mungkin saja melalui e-mail, surat, suara, file, dan banyak lagi. Tanpa dapat dideteksi oleh mesin manapun dan tanpa dapat diblok oleh firewall jenis apapun, social engineer dapat menembus hingga ke data yang sangat penting.

Apakah Sebenarnya Social Engineering?

Apa *sih* arti sebenarnya dari social engineering itu? Bagaimana teknik ini bisa begitu hebat dalam menjebol keamanan informasi dan data Anda? Sebenarnya teknik social engineering tidak lain dan tidak bukan adalah sebuah teknik menipu manusia lain. Tujuannya adalah untuk mendapatkan sesuatu yang diinginkannya. Tidak hanya berupa uang atau harta benda saja, melainkan banyak hal seperti misalnya informasi, kekuasaan, kemenangan, dan banyak lagi.

Aktivitas social engineering dalam dunia TI juga tidak terlepas dari memanipulasi manusia yang berinterksi dengan komputer dengan menggunakan kombinasi dari berbagai teknik seperti memata-matai, mencuri, berbohong, memutar balikkan fakta, dan banyak lagi.

Pelaku penyerangan dengan menggunakan social engineering biasanya tidak memerlukan seperangkat alat-alat canggih atau software yang dapat memecahkan kode-kode sulit. Yang diperlukan dalam proses penyerangan ini adalah pemahaman akan kondisi psikologis dari targetnya, dan tentunya juga kepandaian berbicara.

Siapakah Target Penyerangan dengan Social Engineering Ini?

Yang menjadi target untuk pengganggu keamanan jenis ini sudah barang tentu adalah manusia. Orang-orang yang memiliki sesuatu yang berharga yang dibutuhkan oleh penyerangnya tentulah merupakan target utama. Dalam dunia TI orang-orang yang memiliki informasi penting, baik di kepalanya maupun di komputernya adalah target utama dari social engineering. Tujuannya adalah untuk mengumpulkan informasi penting tersebut namun bukan dari komputernya, melainkan langsung dari penggunanya.

Apa yang Biasanya Dilakukan oleh Penyerang?

Mengumpulkan informasi-informasi penting dari orang lain dapat berupa apa saja. Misalnya mendapatkan informasi *login* dan *password* untuk masuk ke dalam intranet

perusahaannya, menipu pengguna untuk membuka e-mail yang berisi *backdoor* untuk kemudian disinggahi oleh para *hacker*, mencuri data konvidensial seperti misalnya strategi *marketing*, produk baru, dan banyak lagi. Data ini tentu akan sangat berharga sekali bagi orang yang membutuhkannya kelak.

Bagaimana Seseorang Dapat Melakukan Social Engineering?

Para hacker atau penjahat keamanan data yang melakukan social engineering biasanya pandai dalam hal mengerti sifat dan kebiasaan manusia. Selain itu, juga kemampuan untuk membujuk orang lain untuk memberikan informasi merupakan modal dari para hacker jenis ini. Membujuk atau persuasi tersebut sendiri sebenarnya hampir dapat dikategorikan sebagai sebuah seni dan kemudian dipadukan dengan kemampuan teknologi pada kasus social engineering ini.

Sebuah penelitian menunjukan bahwa kebanyakan manusia memiliki beberapa sifat yang cenderung dapat dieksploitasi dengan mudah dengan menggunakan teknik-teknik manipulasi tertentu. Akhirnya dengan menerapkan teknik ini pada manusia tersebut, positif respon akan didapatkan darinya. Dan yang sangat disayangkan banyak juga manusia di antara Anda yang dianugerahi kemampuan dan bakat untuk memanipulasi secara alami, dan tidak sedikit juga yang mempelajarinya untuk tujuan positif maupun negatif.

Para hacker social engineering kebanyakan menggunakan beberapa pendekatan yang hampir sama untuk mendapatkan respon dari target yang sesuai dengan keinginannya. Contoh-contoh pendekatan tersebut adalah sebagai berikut:

- Ketakutan akan kehilangan pekerjaan atau takut menderita karena malu. Biasanya jika seseorang telah berada dalam kondisi ini, maka informasi pribadi yang penting dapat terlepas begitu saja. Setelah memberikan informasi, korban ini akan berharap untuk dapat terlepas dari kondisi yang buruk ini.
- Gengsi, kemewahan, harga diri, dan status dapat merangsang sebuah tindakan membual yang akhirnya akan menyebabkan banyak korban menjadi lengah dan akhirnya melepaskan informasi rahasia yang dimilikinya.
- Para pekerja yang kelebihan beban kerja dan kelelahan dapat dengan tidak sengaja membuat kesalahan. Dan biasanya celah ini dapat dengan mudah dideteksi oleh para hacker yang ingin memanipulasi keadaan ini, seperti contohnya pada saat makan siang, saat akhir pekan, dan banyak lagi.

Beberapa sifat dasar manusia yang dapat mendukung terjadinya proses social engineering dengan mudah adalah terdiri dari enam jenis. Enam sifat tersebut adalah sebagai berikut:

1. Reciprocation (Timbal Balik)

Rasa timbal balik merupakan sifat dasar manusia yang dapat dieksploitasi. Tidak hanya untuk kepentingan social engineering, untuk kepentingan marketing sifat ini pun sering kali digunakan dan kebanyakan berhasil. Biasana jika seseorang telah memberikan sebuah umpan kepada targetnya, maka banyak di antara target tersebut yang tertarik oleh umpan tersebut. Tertariknya dapat disebabkan berbagai alasan. Salah satunya karena rasa timbal balik ini.

Contoh yang paling konkret adalah Anda jadi membeli selusin minuman energi di supermarket hanya karena Anda diberikan satu botol *free sample* dari minuman tersebut. Sering kali hal ini bukan disebabkan karena rasanya yang enak, melainkan karena ada rasa timbal balik yang harus diberikan. Yang memaksa rasa timbal balik ini pun dapat berasal dari berbagai sebab seperti misalnya malu karena sudah menerima free sample, mau mencoba lebih detail, memang rasanya yang disuka, dan banyak lagi. Dari dasar-dasar inilah akhirnya positif respon diberikan oleh target dari social engineering. Meskipun tidak semuanya berhasil, namun persentasenya masih lumayan tinggi biasanya.

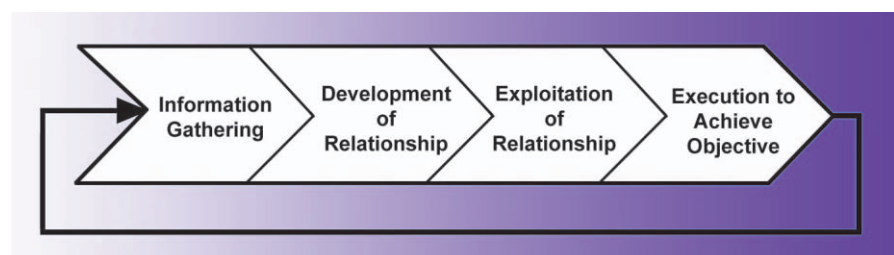
2. Consistency (Konsistensi)

Sikap dan respon manusia terhadap beberapa kejadian yang dialaminya terkadang konsisten dari manusia satu ke manusia lainnya. Misalnya ketika Anda mengajukan sebuah pertanyaan dan kemudian menunggu jawabannya, kebanyakan orang pasti akan merasakan kalau dirinya sedang ditunggu. Sifat-sifat yang mudah ditebak seperti inilah yang dapat digunakan oleh para hacker untuk mengeksploitasi targetnya. Cukup banyak sifat manusia yang konsisten dan mudah di tebak, asalkan para ekploiternya dapat memanipulasi dengan cermat pastilah iya akan mendapatkan apa yang diinginkan dari manusia tersebut.

3. Social Validation (Validasi Sosial)

Social validation merupakan sifat manusia yang sepertinya hampir mendekati bawah sadar atau reflek karena terkadang kita sendiripun tidak menyadari akan melakukan hal tersebut. Sifat social validation merupakan sifat meniru perbuatan seseorang yang dilakukan secara refleks yang sering kali tidak disadari. Sifat mengekor orang ini sebenarnya juga didasari oleh rasa ingin tahu manusianya yang besar akan suatu hal.

Contoh yang paling sering kita jumpai dan alami sendiri adalah kejadian di jalanan. Ketika ada seseorang yang melihat ke satu arah dengan amat serius, maka secara reflek Anda juga pasti akan melihat ke arah yang sama dengan orang tersebut. Hal ini dikarenakan rasa ingin tahu Anda yang sangat besar. Dan juga didorong oleh sifat dasarnya yaitu cenderung mengikuti atau social validation ini. Contoh lain yang sering juga terjadi adalah efek tularan tawa. Jika ada satu orang tertawa dalam sebuah lift yang penuh sesak, meskipun tidak saling kenal mungkin saja pada akhirnya mereka akan tertawa bersama-sama.

Sifat manusia yang seperti ini dapat juga dieksploitasi oleh orang-orang tertentu. Dengan didasari oleh sifat mengekor, para hacker dapat mengirimkan surat berantai atau pesan singkat pada Yahoo! messenger

Proses yang terbilang cukup sederhana dari *social engineering*.

untuk disebarluaskan kepada orang lain. Karena banyak yang melakukan hal tersebut, lama-kelamaan yang tadinya tidak percaya akan isi dari pesan tersebut lama-lama menjadi percaya juga. Pada akhirnya orang tersebut akan terpengaruh untuk mengekor pengiriman email berantai atau pesan Yahoo! messenger tersebut.

Mungkin sebagian dari Anda berpikir apa hubungannya pesan berantai dan pesan Yahoo! messenger dengan keamanan jaringan data Anda. Mungkin para pelakunya tidak bisa mendapatkan data penting dari targetnya. Namun jika targetnya sangat banyak, maka ia sudah hampir berhasil membuat sebuah server yang melayani pengiriman pesan tersebut down. Karena jumlah pesan yang dikirimkannya terus dan terus bertambah, akhirnya kekuatan dari server tersebut teruji juga. Sampai pada batasnya, maka server tersebut akan berhenti bekerja juga.

4. Liking (Kesukaan)

Kebanyakan manusia akan mengatakan kata "ya" atau dengan kata lain setuju pada apa yang mereka sukai. Perlakuan manusia yang seperti ini berlaku pada semua benda dan semua kejadian yang terjadi di muka bumi ini. Salah satu yang paling menonjol adalah sifat suka pada orang-orang yang atraktif, misalnya orang-orang yang cantik, yang dianggap hebat, yang berprestasi, dan banyak lagi.

Atas dasar sifat yang satu inilah terkadang para hacker dapat mengeksploitasi Anda para manusia. Dengan memberikan sebuah umpan yang disuka oleh Anda, maka dengan mudahnya Anda membeberkan informasi pribadi yang sangat rahasia. Cara seperti ini tergolong sangat mudah dilakukan dan tingkat keberhasilannya cukup tinggi.

Sifat manusia seperti ini tidak hanya dimanfaatkan oleh para hacker saja, para *marketer* pun sering memanfaatkan sifat yang satu ini. Misalnya melakukan promosi dengan memasang wanita-wanita cantik dan seksi di depan *counter*, atau memberikan hadiah-hadiah menarik jika Anda membeli beberapa produk mereka, dan banyak lagi.

5. Authority (Otoritas)

Hampir semua orang percaya bahwa jika para ahli dalam suatu bidang yang mengeluarkan pendapat, maka pastilah benar adanya. Para ahli tersebut dianggap seperti pemegang otoritas atau kekuasaan penuh akan pemutusan benar atau salahnya sesuatu. Sifat manusia yang satu ini memang tidak bisa disalahkan karena biasanya kepada siapa lagi mereka akan percaya kalau bukan pada ahlinya atau dengan kata lain orang yang memiliki otoritas.

Celah masuknya para *hacker* yang pandai menggunakan teknis social engineering biasanya ada di antara para staf *call center* dari suatu perusahaan.

Namun lagi-lagi hal ini bisa dieksploit juga, dengan mengatasnamakan para ahli, mereka dapat mengelabui dengan mudah para targetnya, apalagi yang tidak tahu apa-apa sama sekali. Misalnya seorang yang mengaku teknikal support dari sebuah ISP meminta *username* dan *password* login *internet banking* Anda untuk diamankan lebih lanjut. Jika orang yang baru mengerti dalam bidang ini tentu akan percaya bahwa seorang *technical support* itulah ahlinya. Tentu saja pada akhirnya ia sadar bahwa telah tertipu mentah-mentah oleh karena kepercayaannya yang berlebih pada orang yang memiliki otoritas.

6. Scarcity (Kelangkaan)

Sifat dasar manusia yang satu ini memang paling terasa efeknya ketika terjadi. Sifat takut akan kekurangan atau kelangkaan dari sesuatu akan mengakibatkan berbagai hal pada diri manusia, baik itu hal negatif maupun juga hal positif. Paling tidak ada respon yang cukup signifikan dari adanya sifat ini pada manusia.

Takut akan kehabisan cadangan makanan, takut akan kehabisan uang, takut akan kehabisan bahan bakar, takut akan kehilangan pekerjaan yang susah dicari, semua itu adalah ketakutan akan kekurangan atau kelangkaan dari sesuatu. Dan setelah menjadi takut, maka manusia lebih mudah dieksploitasi. Misalnya Anda diancam akan kehilangan pekerjaan yang Anda cintai jika tidak memberikan username dan password dari internet banking Anda, atau jika tidak melakukan suatu hal maka pasokan makanannya akan dihentikan, dan banyak lagi contoh lainnya.

Pada akhirnya manusia akan melakukan segalanya untuk menghindari rasa takut akan kelangkaan atau kekurangan tersebut. Salah satunya adalah dengan memberikan informasi berharga yang diketahuinya. Mudah sekali mengeksploitasinya bukan.

Bagaimana Langkah-langkah Melakukan Social Engineering?

Melakukan social engineering yang notabene hampir sama seperti penipuan biasa juga terdiri dari beberapa step proses. Proses-proses tersebut adalah sebagai berikut:

1. Information Gathering

Proses social engineering yang paling pertama dilakukan adalah mengumpulkan informasi. Para penyerang tersebut memiliki beribu-ribu variasi cara untuk mengumpulkan informasi dari targetnya. Proses ini dapat dilakukan dengan sesederhana mungkin seperti misalnya mengumpulkan informasi dari list telepon, ataupun sampai yang paling sulit dan detail sepertu nomor-nomor jaminan sosial, username password sebuah halaman site, dan banyak lagi.

Proses pengumpulan data ini dapat dijadikan basis untuk membangun hubungan dengan orang lain yang menjadi targetnya. Bahkan setelah Anda mengenal target terkadang informasi secara detail akan datang dengan sendirinya. Semuanya tergantung pada siapa target Anda.

2. Development of Relationship

Adalah sifat manusia yang paling mendasar untuk dapat mempercayai seseorang. Namun apa jadinya jika sifat yang sebenarnya baik tersebut dimanipulasi oleh orang-orang tertentu. Tentunya Anda akan banyak mengalami kesusahan bukan. Begitu pula dengan para hacker yang memanfaatkan jalur ini. Dengan memanfaatkan kepercayaan dari targetnya, ia masuk ke dalam jaringan kehidupan dan bisnis dari targetnya. Terkadang untuk memasukinya pun cukup gampang, hanya tinggal melakukan sesi peneleponan sekali, e-mail, *chatting*, kontak langsung, dan banyak lagi. Intinya setelah kepercayaan yang Anda dapat maka tahap berikutnya adalah informasi rahasia.

3. Exploitation of Relationship

Setelah kepercayaan berhasil Anda dapat dan terjalin hubungan yang baik, langkah berikutnya adalah mulai mengeksploitasi hubungan tersebut. Cara mengeksploitasinya adalah dengan mengorek semua informasi penting yang dimiliki oleh target. Misalnya password, nomor kartu kredit, informasi gaji, informasi strategi penjualan, dan banyak lagi. Selain mengorek informasi, para hacker pada tahap ini juga sudah bisa melakukan aksi-aksinya seperti misalnya membuat account baru pada server, mengubah password milik target tanpa diketahuinya, dan banyak lagi. Tahap pengumpulan informasi atau pelancaran aksi ini dapat dianggap sebagai langkah terakhir ataupun masih dapat digunakan sebagai stage untuk menuju ke proses gangguan keamanan berikutnya.

4. Execution to Achieve Objective

Proses-proses di atas terkadang perlu diulangi berkali-kali untuk mendapatkan suatu hasil yang pas. Maka dari itu, biasanya para hacker akan membuat sebuah siklus pada tahap ini. Siklus ini dapat menjadi umpan bagi proses-proses lainnya agar dapat berjalan dengan baik dan tercapai tujuan dari si penyerang tersebut.

Bagaimana Cara Menanggulangi Serangan Social Engineering?

Sebenarnya bahaya social engineering susah-susah gampang untuk ditanggulangi, karena ini adalah masalah yang disebabkan oleh *human error*, semuanya tergantung pada masing-masing orang yang mengalaminya. Namun tentunya, ada beberapa cara yang dapat memudahkan para target serangan ini untuk mendeteksi dan meminimalisasi kemungkinan terjadinya serangan social engineering. Berikut ini adalah beberapa langkahnya:

1. Buatlah seperangkat peraturan tertulis untuk diikuti oleh para personal Anda yang bertujuan untuk menghalau, mencegah, dan mengurangi serangan social engineering ini. Revisilah selalu peraturan tertulis Anda ini secara berkala agar tidak ketinggalan jaman atau dapat menutup celah-celah baru yang sebelumnya memang tidak ada. Dan jangan lupa untuk selalu mendidik para staf di belakangnya karena staf yang terdidik dengan baik merupakan pertahanan yang kuat bagi serangan ini.
2. Didiklah para customer atau pengguna jasa Anda untuk dapat menerima dan mengikuti segala syarat yang tertulis dalam peraturan tersebut. Sadarkan mereka akan pentingnya prosedur ini untuk menjaga keamanan data dan informasi mereka sendiri.
3. Buatlah sebuah prosedur yang dapat mengeliminasi pertukaran password dan username dalam segala proses. Buat agar semua sistem yang berhubungan dengan password dapat dilakukan secara otomatis dengan program atau perangkat komputer, tanpa adanya perantara manusia dalam keperluan password tersebut. Seperti misalnya membuat program reset password otomatis, halaman penentuan password yang dapat diakses langsung oleh pengguna, dan banyak lagi.
4. Hindarilah penggunaan pertanyaan untuk petunjuk password karena ini juga dapat digunakan para hacker sebagai petunjuk untuk melakukan crack terhadap password Anda. Mereka memiliki berbagai macam cara untuk memecahkan misteri password Anda tersebut dengan sedikit penelitian.
5. Gunakanlah password yang berisikan kata-kata yang tidak biasa diucapkan atau tidak ada relevansinya dengan kehidupan Anda. Misalnya jangan menggunakan tanggal lahir, nama kecil Anda, nama binatang peliharaan Anda, nama anggota keluarga, dan banyak lagi, karena hal ini bisa jadi sangat mudah dapat ditebak oleh penyerang.
6. Jika memungkinkan hilangkan semua elemen manusia pada titik-titik yang penting untuk dijaga keamanannya, seperti misalnya menggunakan sistem token password yang dapat meng-*generate* nomor acak sebagai password, biometric, smard card, sistem *location-based authentication*, dan banyak lagi.

Memalukan, tapi Efektif

Social engineering tidak lain dan tidak bukan sebenarnya adalah sebuah bentuk penipuan biasa. Namun karena sering kali berhubungan dengan dunia TI, maka teknik-tekniknya menjadi cukup populer. Di dalam dunia TI teknik penjebolan keamanan dengan menggunakan cara social engineering memang dianggap paling rendah dan paling memalukan untuk dilakukan. Namun pada kenyataannya, teknik inilah justru yang paling cepat dan efektif dilakukan. Anda tidak perlu repot-repot belajar bahasa pemrograman atau menguasai firewall dari perangkat-perangkat jaringan target Anda. Yang dibutuhkan hanylah kemampuan untuk memanipulasi perkataan dan juga pikiran orang menjadi sesuai dengan yang Anda inginkan.

Maka dari itu, teknik pengganggu keamanan jaringan data Anda yang satu ini paling sulit untuk dideteksi dan dikontrol, karena tidak ada parameter bakunya yang benar-benar visibel untuk dimonitor. Semua berbalik lagi kepada Anda yang memiliki informasi penting tersebut. Apakah Anda begitu mudahnya tertipu oleh akal-akalan para penyerang? Siapkanlah diri Anda! ■

Lebih Lanjut

- **http://www.gartner.com/gc/webletter/security/issue1/article2.html**
- **http://www.gartner.com/gc/webletter/security/issue1/article1.html**
- **http://www.gartner.com/gc/webletter/security/issue1/index.html**
- **http://software.silicon.com/security/0,39024655,39125919,00.htm**

Hermawan Sutanto

Saatnya Upgrade ke SQL Server 2005?

Dihadirkan sebagai *platform* manajemen data yang sangat komprehensif, SQL Server 2005 mengemas fitur-fitur seperti sistem manajemen data relasional, *data warehousing*, sampai BI (*business intelligence*). Apakah ini saatnya untuk *upgrade* ke SQL Server 2005?

Sebelum kita beranjak lebih jauh, maka perlu dicermati alasan-alasan apa saja yang bisa dijadikan sebagai bahan pertimbangan untuk melakukan *upgrade* atau bermigrasi ke SQL Server 2005.

Ketatnya persaingan bisnis saat ini menuntut perusahaan untuk menerapkan solusi manajemen data yang komprehensif dan dapat memberikan hasil semaksimal mungkin secara efisien. Fitur-fitur manajemen data yang lengkap dan terintegrasi dengan baik adalah kunci untuk mencapai harapan tersebut.

Lebih dari sekadar mengelola data relasional, maka solusi manajemen data yang ideal juga harus melengkapi dirinya dengan kemampuan untuk melakukan integrasi data—umumnya dikenal sebagai proses ETL (*extraction, tranformation, and loading*), kemampuan untuk menganalisis data, dan diakhiri dengan kemampuan untuk menyajikan hasil pengolahan data tersebut sebagai informasi yang bernilai tambah.

Di sinilah SQL Server 2005 mencoba untuk memposisikan dirinya, dengan menyertakan fitur-fitur yang dibutuhkan untuk memainkan peran dalam siklus manajemen data: *manage, integrate, analyze, and report.* Selain itu, agar dapat "bermain" di tingkat *enterprise*, SQL Server 2005 juga didesain untuk memberikan tingkat keamanan, kinerja, dan *availability* yang dapat memenuhi kebutuhan aplikasi skala enterprise.

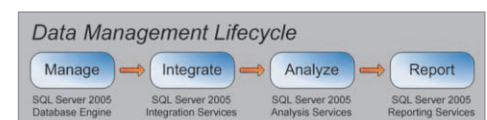
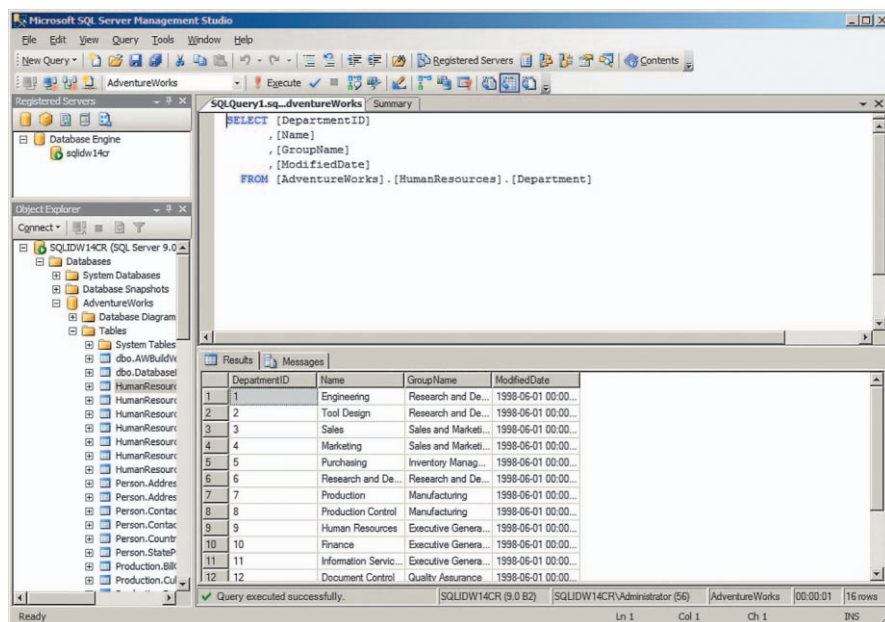
Platform Manajemen Data yang Enterprise-Ready

Berbicara mengenai *platform* manajemen data skala enterprise, maka ada sejumlah kriteria yang harus dipenuhi, yaitu kinerja, availability, *manageability*, keamanan, dan skalabilitas.

Platform manajemen data berbasis teknologi SQL Server 2005 menjanjikan peningkatan kinerja pada setiap komponennya, mulai dari *relational engine* yang dapat melayani tuntutan kerja OLTP yang sangat tinggi dan data *warehouse* berukuran multi-terabyte, kemampuan ETL—dikenal dengan nama SQL Server 2005 Integration Services (SSIS)—yang dapat memindahkan jutaan *record* per detik saat melakukan transformasi data di memory, sampai sistem OLAP (*online analytical processing*)—menggunakan SQL Server 2005 Analysis Services—yang dapat melakukan *query* dalam hitungan sub-*second* dan melakukan data mining terhadap dataset yang berukuran sangat besar. Sedangkan untuk kemampuan pelaporannya, menggunakan SQL Server 2005 Reporting Services, dapat di-*deploy* secara sangat fleksibel (bisa di-*scale out* atau di-*scale up*) dan memiliki fitur-fitur seperti *advanced caching* dan *snapshot* untuk mendukung tingkat *concurrency* penggunaan oleh banyak user.

Dalam urusan menjaga availability terhadap data yang digunakan oleh aplikasi-aplikasi yang sifatnya *mission-critical*, SQL Server 2005 memiliki kemampuan untuk melakukan *failover clustering* dan *database mirroring*. Fitur-fitur seperti online *indexing, partitioning, dynamic configuration,* dan *hot memory swapping*, serta kemampuan untuk melakukan *back-up* dan *restore* terhadap sebagian data tanpa perlu mematikan keseluruhan database, akan dapat mengurangi atau meniadakan *downtime* sehingga user dapat mengakses data tanpa gangguan. Komponen SSIS pun mendapat perhatian khusus dalam menjaga availability-nya, di mana *deployment*-nya dapat didistribusikan ke sejumlah server sehingga tidak ada *single point of failure* dalam proses ETL. Komponen SQL Server 2005 Analysis Services memiliki kemampuan server-sync sehingga memungkinkan sejumlah server cadangan untuk mendukung server utama dalam melakukan proses OLAP. Demikian halnya dengan komponen SQL Server 2005 Reporting Services yang diintegrasikan dengan IIS (Internet Information Services), di mana dapat memanfaatkan kemampuan NLB (*Network Load Balancing*) dari IIS untuk meningkatkan tingkat *uptime* dari sistem pelaporan. SQL Server 2005 juga menyediakan fitur DAC (*dedicated administrator connection*) yang dapat digunakan untuk mengakses suatu *instance* dari SQL Server 2005 secara langsung untuk melakukan pemulihan saat database mengalami gangguan.

Sebagai usaha untuk meningkatkan manageability, SQL Server 2005 menggunakan satu unified management tool—SQL Server Management Studio, di mana keseluruhan sistem manajemen data berbasis SQL Server 2005 dapat dikelola melalui satu antarmuka saja. Selain itu, keadaan dari seluruh komponen inti SQL Server 2005 (SQL Server Database Services, Analysis Services, dan Integration Services) dapat dipantau oleh SQL Server Profiler, sehingga dapat mempermudah pengidentifikasian, *troubleshooting*, dan penanganan masalah kinerja—dengan bantuan Database Tuning Wizard (DTA). Sedangkan untuk otomatisasi tugas-tugas administratif yang bersifat umum dan repetitif, dapat dilakukan dengan menggunakan SMO (SQL Management Objects) dan Profiler API.

Lahir sebagai produk yang dikembangkan saat Microsoft mulai menggencarkan inisiatif Trustworthy Computing, maka SQL Server 2005 menganut filosofi *secure by design, secure by default, and secure in deployment*. Alhasil, secara default SQL Server 2005 akan terinstal dalam keadaan "terkunci", dan selanjutnya tingkat keamanannya dapat di-*configure* sesuai kebutuhan menggunakan

SQL Server 2005 sebagai *platform* manajemen data yang komprehensif.

SQL Server Management Studio sebagai *unified management tool.*

Surface Area Configuration (SAC). Pengaturan hak administratif SQL Server 2005 juga dapat dilakukan secara lebih mendetail, sehingga hak-hak administratif dan pengembangan aplikasi database dapat dipisahkan dari tingkatan hak akses data di setiap subkomponen dari SQL Server 2005. Tak luput adalah peningkatan kemampuan enkripsi data dalam penyimpanan maupun saat ditransmisikan, dan juga lingkungan pengembangan aplikasi yang lebih aman.

Di sisi skalabilitas, platform manajemen data berbasis teknologi SQL Server 2005 menjangkau mulai dari perangkat handheld dengan SQL Server 2005 Mobile Edition-nya, sampai ke sistem OLTP (*online transactional processing*) dan data warehouse yang mengelola data dalam ukuran multi-terabyte—menggunakan SQL Server 2005 Enterprise Edition.

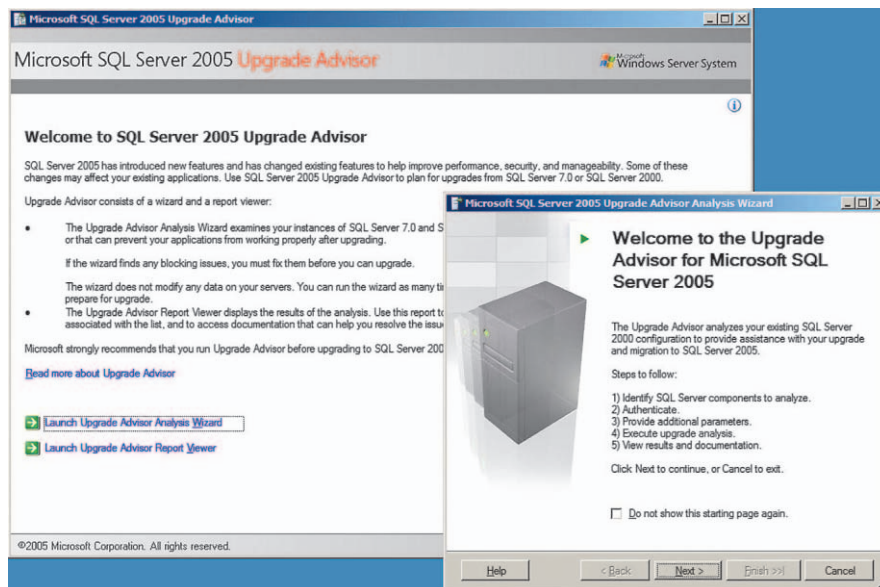
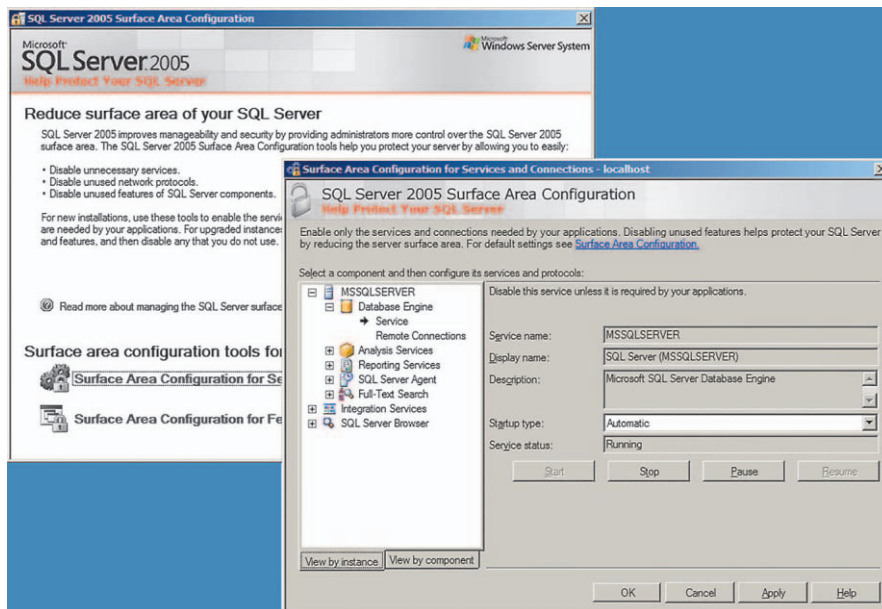
Mempersiapkan Diri untuk Melakukan Upgrade

SQL Server 2005 memungkinkan dilakukannya upgrade secara langsung dari SQL Server 2000 atau SQL Server 7.0. Selain melakukan upgrade, perpindahan ke SQL Server 2005 juga bisa dicapai melalui proses migrasi.

Perbedaan di antara keduanya adalah bahwa upgrade merupakan proses terotomatisasi, di mana instance lama dari SQL Server akan dipindahkan ke instance baru—dan tetap mempertahankan data dan metadata dari instance lama tersebut. Sedangkan migrasi adalah proses manual, di mana DBA (database administrator) membuat instance baru dan menyalin data dan metadata ke instance baru tersebut. Hasil dari proses migrasi adalah bahwa terdapat dua instance dari data yang sama, sehingga DBA bisa melakukan verfikasi dan perbandingan antara kedua instance yang menggunakan sistem yang berbeda tersebut, sebelum pada akhirnya memindahkan aplikasi yang ada ke instance baru yang menggunakan SQL Server 2005.

Untuk membantu proses upgrade, maka disediakan Upgrade Advisor yang akan menganalisis konfigurasi dari server database, services yang berjalan, dan aplikasi yang ada saat ini, untuk kemudian memberikan laporan mengenai perubahan apa saja di SQL Server 2005 yang akan mempengaruhi proses upgrade yang ingin dilakukan.

Upgrade terhadap database engine adalah yang paling mudah untuk dilakukan, dan akan memberikan manfaat secara langsung di bidang kinerja, availability, dan manageability. Seluruh aplikasi yang menggunakan Microsoft Data Access Components (MDAC) dan ADO. NET akan berfungsi tanpa masalah, seperti saat sedang dijalankan di atas SQL Server 2000 atau SQL Server 7.0. Apabila ingin memanfaatkan fitur-fitur baru di SQL Server 2005, seperti MARS (Multiple Active Result Sets), tipe data XML, dan user-defined types (UDTs), aplikasi harus dimodifikasi untuk memanfaatkan SQL Native Client yang baru hadir di SQL Server 2005 ini. Patut dicatat bahwa saat melakukan upgrade, maka compatibility mode dari SQL Server 2005 akan diset ke versi 8.0 (yaitu SQL Server 2000), di mana akan membantu *stored procedure* yang ada sebelumnya agar tetap dapat berfungsi, walau referensi T-SQL yang digunakan sudah tidak lagi didukung oleh SQL Server 2005.

Komponen ETL di SQL Server 2005—SQL Server 2005 Integration Services (SSIS) merupakan komponen baru yang benar-benar ditulis dari awal tanpa membawa satu kode pun dari tool ETL yang ada di versi sebelumnya, yaitu *Data Transformation Services* (DTS). Karena perubahan yang sangat mendasar di sisi arsitektur, peralihan dari DTS ke SSIS merupakan proses migrasi, yang akan dibantu oleh

Tampilan layar SQL Server 2005 Upgrade Advisor.

Surface Area Configuration untuk mengamankan server database yang menjalankan SQL Server 2005.

wizard dalam beberapa hal, akan tetapi tetap membutuhkan desain ulang secara manual untuk menyelesaikan proses migrasi tersebut. Sementara DTS package dimigrasikan ke SSIS, ada opsi saat instalasi SQL Server 2005 yang memungkinkan kita agar tetap dapat menjalankan DTS package di SQL Server 2005. Dengan kemampuan ini, maka proses migrasi dapat dilakukan secara perlahan dan tetap mempertahankan fungsionalitas dari solusi ETL yang sudah dikembangkan sebelumnya.

Seluruh kekuatan dari Analysis Services di SQL Server 2000 tetap dipertahankan di SQL Server 2005, dan mendapat penambahan fitur baru seperti Unified Dimensional Model (UDM) serta sejumlah peningkatan pada fitur-fitur lama. Di sisi upgrade, perpindahan dari Analysis Services 2000 ke Analysis Services 2005 dapat dilakukan secara mudah—dengan tetap mempertahankan *cube, partition, dimension hierarchy, measure, calculation,* dan set yang ada. Akan tetapi, Migration Wizard yang disediakan tidak akan mengoptimalkan objek-objek Analysis Services lama tersebut, karena tujuan utamanya agar aplikasi lama yang bergantung kepada struktur Analysis Services 2000 tidak terganggu. Walau demikian, cube yang dimigrasikan ke Analysis Services 2005 akan dapat secara langsung memanfaatkan peningkatan kinerja dan skalabilitas dari arsitektur Analysis Services yang baru tersebut.

Perubahan-perubahan di Analysis Services 2005 yang perlu menjadi bahan pertimbangan saat melakukan upgrade adalah pada metode akses oleh aplikasi client dan perubahan struktur yang berdampak pada pembuatan laporan dari data OLAP. Analysis Services 2005 menggunakan protokol Web services untuk OLAP, yaitu XML for Analysis (XML/A). Untuk memanfaatkannya, komponen client OLEDB for OLAP (Pivot Table Services—PTS) harus di-*update* dengan versi PTS yang disertakan oleh SQL Server 2005. Sedangkan perubahan struktur OLAP di Analysis Services 2005 dapat menyebabkan *query* MDX (multidimesional expression) yang ada sebelumnya tidak berfungsi semestinya, sehingga laporan-laporan yang dibuat berdasarkan MDX harus dibuat ulang untuk menyesuaikan dengan struktur OLAP baru di Analysis Services 2005.

Khusus untuk komponen SQL Server 2005 Reporting Services, tidak ada perubahan signifikan di sisi arsitektur dari versi sebelumnya, karena Reporting Services 2000 sendiri baru dirilis pada tahun 2004. Akan tetapi, ada sejumlah fitur baru seperti multi-select parameters, dukungan MDX secara *built-in,* dan dynamic report generation. Definisi laporan berbasis RDL (*Report Definition Language*) yang dibuat menggunakan Reporting Services 2000 dapat dijalankan secara langsung tanpa perlu di-upgrade. Akan tetapi, saat sebuah laporan dibuka menggunakan BI Development Studio yang menjadi bawaan dari SQL Server 2005, maka developer akan diminta untuk mengonversi RDL yang lama ke versi baru yang sesuai dengan standar Reporting Services 2005.

Di sisi *hardware*, dukungan terhadap platform komputer berbasis teknologi 64-bit dari Intel (Intel Itanium 2 dan Intel EMT64) dan AMD (AMD x64), membuka peluang sebesar-besarnya bagi SQL Server 2005 untuk memanfaatkan hingga 128 prosesor dan memory sebesar 512GB dalam satu server, sehingga dapat menangani beban kerja pemroresan data yang sangat tinggi. Peralihan dari SQL Server versi 32-bit ke 64-bit pun dapat dilakukan secara mudah, karena keduanya menggunakan struktur penyimpanan data yang sama. Dengan demikian, migrasi ke teknologi 64-bit dapat dilakukan semudah men-*detach* database dari sistem 32-bit dan kemudian meng-*attach*-nya ke sistem 64-bit.

Kesimpulan

Kehadiran SQL Server 2005 yang sudah ditunggu-tunggu oleh sebagian kalangan patut disambut secara gembira—karena akhirnya menghadirkan fitur-fitur canggih yang menjadikannya sebagai platform manajemen data yang komprehensif dan *enterprise-ready.*

Konsolidasi komponen-komponen pendukung siklus manajemen data yang lengkap (*manage, integrate, analyze, and report*) di SQL Server 2005 secara tidak langsung akan mengurangi TCO (*total cost of ownership*), karena efisiensi dan efektivitas yang lebih tinggi dapat dicapai melalui penyederhanaan sumber daya (hardware, software, dan orang) yang diperlukan untuk mendukung solusi manajemen data tersebut.

Apabila diputuskan untuk melakukan upgrade ke SQL Server 2005, lakukanlah secara hati-hati dan terapkan proses *change management* yang baik. Pecahlah proses upgrade ke dalam sejumlah fase, mulai dari *planning and research, testing and process validation, production upgrade,* sampai *post-upgrade considerations.* Gunakanlah SQL Server 2005 Upgrade Advisor dan Setup Wizard untuk membantu menghindari "kejutan" yang akan terjadi saat melakukan upgrade, dan untuk mengidentifikasi area-area yang perlu mendapat perhatian khusus.

Setelah upgrade berhasil dilakukan secara mulus dan tanpa kendala yang berarti, Anda akan siap mengeksploitasi seluruh kemampuan yang bisa diberikan SQL Server 2005. ■

Lebih Lanjut

- **http://www.microsoft.com/sql/solutions/upgrade/default.mspx**

Gunung Sarjono

Pengambil Data

Anda telah men-*scan* dengan program anti-*spyware* dan menemukan pengambil data pada PC Anda. Apakah mereka berbahaya?

Scan sistem Anda untuk menghilangkan *spyware* dan kemungkinan besar Anda akan menemukan pengambil data atau *adware*. Meskipun mereka jauh lebih sering dijumpai dibanding *keystroke logger*, apakah mereka sama bahayanya? Setiap *form* yang Anda isi (*online* atau tidak, survai yang diselesaikan dan informasi yang diberikan berisi informasi berharga. Perusahaan pengambil data melakukan pengamatan data untuk menemukan potongan informasi yang menunjukkan minat dan kesukaan pribadi Anda dengan harapan menggunakan informasi tersebut untuk memasarkan produk atau jasa kepada Anda—terutama, yang mungkin Anda suka.

Pengambilan data pada Internet bekerja dengan cara yang sama, tetapi terutama berfokus pada pemantauan aktivitas *surfing* online Anda. Sebagai contoh, jika seseorang mempunyai daftar situs web yang Anda kunjungi selama seminggu, mereka bisa mengetahui bahwa Anda menyukai golf, otomotif, dan bahkan liburan di Bali. Ini mungkin tidak begitu berbahaya, tetapi di balik semua itu terdapat masalah privasi.

Scanning Spyware dan Adware

Untuk men-scan pengambil data dengan Ad-Aware SE, buka Ad-Aware SE dan klik 'Check for updates now'. Pada jendela Performing WebUpdate, klik tombol Connect. Setelah update program di-*download* dan diinstalasi, klik Finish. Klik Next untuk mengonfigurasi *setting* scan. Pada layar Preparing System Scan, klik 'Perform full system scan'. Opsi ini akan men-scan drive pada harddisk dan lebih komprehensif dibanding opsi *smart scan*. Klik Next untuk memulai scanning. Setelah scanning selesai, beri tanda centang (✓) pengambil data atau spyware yang ditemukan dan kemudian klik Next. Pada waktu ditanya, klik OK. Sistem Anda sekarang bebas dari pengambil data (yang ditemukan).

Contoh Pengambil

Setelah men-scan spyware, Anda akan mendapatkan sejumlah pengambil data. Mereka masuk ke PC dengan berbagai cara, tetapi kebanyakan melalui instalasi program dan surfing web sehari-hari. Pengambil data yang berasal dari surfing web biasanya datang dalam bentuk *cookie*, sedangkan yang berasal dari instalasi sofware sedikit lebih licin; biasanya Anda telah setuju untuk menginstalasi komponen tersebut pada PC, dan mungkin tanpa Anda sadari.

Bagaimana suatu software diinstalasi tanpa seizin Anda? Jawabannya sederhana: semua terjadi melalui perjanjian lisensi. Tersembunyi di balik semua teks tersebut adalah pernyataan sebab-akibat, 'If you accept this agreement and install this program, you also agree to have XYZ's data mining objects installed on your PC'. Ini merupakan salah satu alasan mengapa kita harus membaca perjanjian tersebut dengan saksama, terutama pada waktu menginstalasi program (apalagi yang *free*) dari sumber yang tidak dikenal.

Namun, mengapa seseorang ingin mengawasi aktivitas surfing Anda? Itu karena apa yang Anda lakukan pada waktu online merupakan harta karun data *marketing*. Beberapa tool pengambil data (seperti toolbar Alexa) mengumpulkan detail surfing untuk menyusun rating situs web. Pengambil data yang lain mengumpulkan daftar situs web yang Anda kunjungi dan iklan yang Anda klik, dan kemudian menggunakan informasi tersebut untuk mengirimkan penawaran khusus, spanduk iklan dan e-mail kepada Anda yang disesuaikan dengan minat Anda. Banyak pengambil data yang menjual data Anda kepada pihak ketiga yang akan menggunakan data tersebut sesuka mereka. Ini semua sangat licik, terutama pada waktu masalah privasi tidak dinyatakan secara jelas.

Anda juga mungkin ingin tahu mengapa situs web menggunakan jasa spanduk iklan atau menyertakan komponen pengambil data pada *software* mereka. Jawabannya adalah uang. Situs yang meng-*hosting* spanduk tersebut biasanya mendapatkan uang per klik, dan mendapatkan persentase dari hasil penjualan, atau menerima pembayaran dari perusahaan yang ingin mendapatkan data yang diambil.

Masalah Privasi

Kita semua dibombardir dengan iklan setiap harinya. Oleh karena itu, banyak orang memilih untuk tidak mempedulikan iklan online. Banyak yang tidak sadar bahwa pengambilan

Manajemen Cookie

■ Salah satu cara yang paling sering digunakan iklan online untuk mengawasi kebiasaan *browsing* Anda adalah dengan menggunakan *cookie*. File ini menyimpan informasi tentang situs web yang Anda kunjungi dan informasi lainnya seperti waktu, tanggal, dan seterusnya. Hal ini membuat citra cookie menjadi jelek, tetapi tidak semua mengawasi aktivitas online Anda. Pada kenyataannya, banyak yang berguna. Sebagai contoh, cookie bisa digunakan untuk menyimpan informasi tentang preferensi pribadi Anda pada suatu situs Web tertentu, atau digunakan supaya Anda tidak perlu memasukkan *username* dan *password* setiap kali mengunjungi situs yang aman. Oleh karena itu, yang perlu Anda lakukan adalah memisahkan dari cookie yang berguna tersebut dari yang mengawasi aktivitas online Anda.

Pada Internet Explorer dan Firefox, buka Tools, Internet Options, Privacy untuk mengonfigurasi *setting* cookie. Jika Anda ingin solusi yang lebih andal, coba gunakan CookieWall. Program ini secara *real time* akan menanyakan Anda apakah memperbolehkan atau menolak cookie, dan juga memungkinkan Anda untuk mengonfigurasi setting cookie keseluruhan sistem. Cookie pada dasarnya tidak membahayakan PC, tetapi bisa mempengaruhi privasi Anda. Sebaiknya Anda simpan cookies dari situs yang aman dan menolak semua yang lain.

Mengejar Keylogger

■ Jika komputer Anda terinfeksi keylogger, menghapusnya dengan program seperti Microsoft AntiSpyware hanya langkah pertama dalam proses pembersihan. Jika keylogger sudah lama berada pada PC Anda, maka kemungkinan besar satu atau beberapa orang sekarang mempunyai akses ke sebagian informasi pribadi Anda, termasuk username dan password.

Setelah menghapus keylogger, reboot dan lakukan pemeriksaan lagi untuk memastikan keylogger telah hilang selamanya. Setelah itu, ganti semua password Anda—yang berhubungan dengan *e-mail account, online banking,* program *instant messaging*, situs lelang online, dan seterusnya. Meskipun orang yang menginstalasi keylogger hanya ingin memata-matai aktivitas berkomputer Anda, bisa saja mereka juga mengejar detail user account. Dengan mempunyai informasi yang cukup, mencuri identitas (belum lagi uang Anda) adalah pekerjaan mudah.

Anda harus memikirkan bagaimana program tersebut awalnya bisa masuk. Apakah user lain menginstalasinya? Apakah di-*download* dari Internet? Apakah Anda mempunyai firewall, antivirus, dan anti-spyware telah di-*update* dan melindungi Anda sepanjang waktu? Hal positif dari keylogger adalah peningkatan kewaspadaan keamanan yang disebabkannya. Tidak seorang pun suka dimata-matai, jadi lakukan tindakan yang diperlukan untuk memastikan keylogger tidak lagi masuk ke komputer Anda.

data terjadi juga, sementara yang lain memilih untuk mengabaikannya. Namun, perlu diketahui bahwa objek tersebut dan mekanisme *tracking* mengancam privasi Anda. Meskipun obyek tersebut digunakan untuk keperluan marketing, bukan tidak mungkin mereka akan digunakan untuk hal negatif pada masa mendatang. Bayangkan jika Anda mulai menerima surat atau telepon mengusik Anda mengenai situs yang dikunjungi, atau bahkan mengancam akan memeras Anda—kemungkinannya tidak enak untuk dipikirkan.

Kata Terakhir

Pada akhirnya, pengambil data tidak menunjukkan secara jelas sebagai ancaman yang serius ke sekuriti komputer Anda. Kemungkinannya kecil infomasi yang dikumpulkan oleh mereka digunakan untuk mengancam Anda (atau PC Anda). Namun, mereka menunjukkan invasi superior terhadap privasi surfing Anda. Jika tidak ingin menjadi target penerima e-mail sampah, spanduk iklan dan sejenisnya maka mereka sebaiknya dihilangkan bersama dengan spyware. Tidak ada seorang pun yang suka diawasi, meskipun pada dasarnya pengambil data tidak menjadi ancaman yang serius sekarang, itu bukan berarti mereka tidak membahayakan nantinya. Sebaiknya, apapun yang mengawasi aktivitas online Anda harus dibuang.

Keylogger

Bagaimana perasaan Anda jika tahu ada seseorang di luar sana yang bisa membaca setiap kata yang Anda ketik, termasuk e-mail, password, dan percakapan IM? Mungkin sangat tidak nyaman, tetapi itu bisa dan memang terjadi melalui keylogger. Begitu terinstalasi pada PC Anda, orang yang menginstalasinya benar-benar bisa melihat setiap tombol yang Anda tekan—yang baik, jahat, dan jelek.

Keystroke logger atau disingkat keylogger, sering dihubungkan dengan kegunaannya sebagai tool terlarang atau jahat yang diinstalasi secara diam-diam untuk mengambil semua tombol yang ditekan. Sama seperti tool hacker lainnya, keystroke logging dimaksudkan sebagai tool administrasi dan diagnosis. Sayangnya, beberapa dari tool dan utility tersebut digunakan untuk kejahatan.

Keylogger adalah produk *hardware* atau utility software yang mencatat semua penekanan tombol pada komputer. Bisa saja hanya mencatat penekakan tombol dan datanya diambil secara manual, atau didesain supaya otomatis mengirimkan hasilnya ke suatu alamat e-mail. Keylogger hardware biasanya suatu perangkat yang dipasang di antara komputer dan keyboard. Pengguna yang teliti atau waspada bisa memeriksa dan menemukan keylogger semacam ini. Namun, beberapa keylogger hardware lebih tersembunyi dan bisa saja dimasukkan ke dalam keyboard itu sendiri supaya tidak diketahui.

Keylogger software biasanya terdiri dari dua file yang diinstalasi pada direktori yang sama: DLL yang melakukan semua pekerjaan

Mencegah Serangan Keylogger

■ Berikut adalah lima cara yang dapat Anda lakukan untuk mendeteksi spyware dan pencegahannya:

1. Instalasi filter spyware pada host. Banyak scanner spyware yang tersedia di pasaran. Jika Anda mencari solusi yang tidak terlalu mahal, coba gunakan tool beta Microsoft, Windows Spywares, Spybot, dan AdAware. Banyak vendor antivirus komersial, seperti McAfee, juga mempunyai filter spyware yang digabungkan ke dalam solusi antivirus korporat.
2. Instalasi suatu aplikasi *gateware* dengan fitering *content* spyware. Jika tadi pada tingkat host, maka sekarang kita lihat solusi spyware yang beroperasi pada tingkat jaringan. Salah satunya dalah Blue Coat Spyware Interceptor. Jika anggaran Anda mencukupi, pertimbangkan untuk menggunakan solusi ini.
3. Buat egress filter pada jaringan Anda. Tidak ada salahnya untuk membuat filter egress pada jaringan. Mereka bisa membantu dalam memblokir spyware yang mencoba "menelpon rumah".
4. Monitor intrusion-detection system (IDS) Anda dan jaga *signature* tetap terbaru. Jika Anda tidak bisa memblokir spyware dari menelpon rumah, paling tidak Anda bisa mendeteksinya dengan IDS dan menggunakan laporannya untuk mengidentifikasi sistem yang terinfeksi.
5. Cegah user menginstalasi software *download*. Kebanyakan instalasi spyware disebabkan oleh user yang menginstalasi sofware yang di-download dari Internet. Jika memungkinkan awasi aktivitas tersebut.

Spyware dan pengambil data yang sejenis merupakan salah satu tantangan paling penting yang dihadapi oleh profesioal sekuriti informasi. Sudah saatnya memastikan organisasi Anda dalam keadaan aman. Dengan mengikuti langkat di atas akan membantu Anda dalam mencapai tujuan tersebut.

Egress Filter

■ Jika sudah cukup lama bergelut dengan router dan firewall, Anda mungkin tidak asing lagi dengan konsep ingress filtering—penggunaan firewall untuk mengatur *traffic inbound.* Ingress filtering memungkinkan Anda untuk mengontrol traffic yang masuk ke jaringan dan membatasi aktivitas. Anda mungkin tidak familiar dengan cara sekuriti yang sama yang dikenal dengan *egress filtering*, yang mengontrol traffic yang keluar dari jaringan Anda. Penambahan aturan ke router dan/atau firewall memungkinkan Anda untuk memberikan perlindungan dari tindak kejahatan yang banyak terjadi. Dua aturan yang bisa diimplementasikan adalah tidak ada outbound yang memuat alamat IP yang bukan untuk jaringan Anda (Ini merupakan aturan dasar egress filtering), dan tidak ada yang memuat alamat IP privat (non-routable). (Kenyataannya memang demikian, tetapi tidak ada salahnya memblokir dan mencatat traffic ini untuk mengetahui sumber error).

Seiring dengan kontrol sekuriti, pengecualian terhadap egrees filter perlu dilakukan bergantung pada kebutuhan organisasi Anda. Aturan ini harus digunakan sebagai dasar kebijakan dan perlu dibuat pengecualian untuk mendukung kegiatan bisnis.

Mengapa kita harus peduli terhadap egress filtering? Lagipula, itu bukan perimeter yang aman untuk mencegah masuknya traffic yang mencurigakan? Sederhana saja, egress filtering umumnya perlu dilakukan. Dengan melakukan itu, Anda bisa mencegah penggunaan jaringan untuk melakukan serangan *denial-of-service* (DDoS) ke suatu situs Internet. Jika situs Anda digunakan untuk melakukan serangan tersebut, maka paling tidak Anda mengganggu administrator sekuriti lain. Yang terburuk, Anda bisa dianggap melanggar hukum meskipun sebenarnya tidak melakukan hal yang salah!

Aturan egress filtering juga sama dengan ingress filtering. Tidak ada traffic inbound yang memuat alamat IP yang diberikan untuk jaringan Anda. Tidak ada traffic inbound yang memuat alamat IP privat (non-*routable*). Aturan ini sudah biasa, tetapi seringkali dilupakan oleh administrator pada waktu membuat aturan yang kompleks yang membatasi aktivitas berdasarkan port. Hanya butuh beberapa menit untuk membuat aturan tersebut ke perangkat pengaman Anda dan mereka bisa mencegah terjadi serangan DDoS yang dilakukan dari tempat Anda.

dan EXE yang memuat DLL tersebut. Yang sederhana sering kali dijalankan pada waktu *booting* melalui registry. Yang lebih canggih tidak terlihat dalam daftar proses dan bisa beroperasi pada tingkat kernel serta entri registry-nya tidak terlihat. Terlepas dari bentuk mereka, keylogger dimaksudkan untuk mengawasi apa yang Anda ketik pada komputer sehingga dapat dilihat oleh pihak lain.

Mereka sudah lama ada, tetapi keylogger mulai mendapatkan perhatian serius. Ini terutama karena banyak spyware yang menyertakan keylogger, yang memungkinkan semua yang Anda ketik dikirimkan ke seseorang di Internet. Namun, keylogger kadang-kadang sengaja diinstalasi untuk mengawasi aktivitas PC para karyawan dan anak-anak. Suka atau tidak suka (bergantung apakah Anda pelakunya atau korban), keylogger merupakan ancaman serius terhadap sekuriti komputer dan privasi pribadi Anda.

Meskipun sering dihubungkan dengah hal jahat, keylogger kadang digunakan. Beberapa organisasi menginstalasi mereka pada komputer karyawan yang dicurigai mencuri atau aktivitas tidak etis lainnya. Sama juga, banyak orang tua menggunakan program ini untuk mengawasi aktivitas online anak mereka supaya tidak mengunjungi situs yang tidak pantas atau berhubungan dengan hal yang berbahaya. Tentu saka, batas etis terhadap pengintaian semacam ini menjadi kabur. Pada beberapa yurisdiksi, pemilik mempunyai hak absolut untuk mengawasi penggunaan komputer para karyawan. Hal yang sama berlaku untuk orang tua yang perhatiannya tinggi, seperti menjaga anak mereka supaya aman pada waktu online.

Dari Mana Keylogger Datang?

Sekarang ini, program keylogger komersial digunakan sebagai tool untuk memata-matai orang lain, memastikan rekannya setia, dan mengawas bagaimana yang lain menggunakan PC Anda. Vendor software keylogger memasarkan produk mereka sebagai tool anti pencurian dan keamanan anak. Salah satu contohnya adalah Blazing Tools Perfect Keylogger.

Keylogger yang legal hanya melakukan persentase kecil dari keylogger yang berada pada komputer orang-orang. Ratusan ancaman spyware meliputi keylogging. Dimaksudkan untuk mencuri username, password, dan bahkan identitas Anda, program ini biasanya diinstalasi tanpa sepengetahuan Anda, dan sering kali bersamaan dengan program lain yang sah. Beberapa orang jahat tertentu bahkan mengemas keylogger dengan program anti-spyware dan kemudian menjajakan mereka sebagai solusi penghapus spyware. Apapun yang terjadi di Internet, dan kadang-kadang Anda mendapatkan lebih dari yang diharapkan dari program *free*. Anda harus selalu mengecek asal program yang diinstalasi untuk memastikan Anda menerima versi yang sah.

Mengapa Keylogger Berbahaya?

Keylogger berbahaya karena beberapa alasan. Pertama dan terutama, mereka memungkinkan user lain untuk memata-matai penggunaan komputer Anda, di mana ini sangat tidak etis. Selanjutnya adalah masalah privasi. Keylogger jahat hampir selalu terhubung langsung untuk mencuri detail user account seperti username dan password. Dengan diketahuinya detail Anda, orang yang mencatat penekanan tombol bisa mengakses rekening bank, e-mail Anda, dan pada akhirnya mencuri identitas Anda.

Cari dan Hapus Mereka

Mencari dan menghapus keylogger spyware dan komersial biasanya tidak terlalu sulit, karena kebanyakan program anti-spyware bisa melakukan itu. Namun, Anda bisa saja menemukan keylogger dan tidak bisa menghapusnya karena tidak mempunyai hak akses administrator. Jika ini terjadi, bicaralah kapada orang yang mengurus komputer Anda. Mungkin saja program tersebut diinstalasi oleh spyware, tapi Anda akan mengetahui alasan mereka diinstalasi. Jika keylogger sengaja diinstalasi, tanyakan mengapa ada di situ. Tidak seorang pun yang suka dimata-matai dan jika itu terjadi pada Anda, bukan tidak beralasan untuk meminta agar tindakan itu dihentikan. ■

Lebih Lanjut

- **http://www.analogx.com/contents/download/network/cookie.htm**
- **http://www.blazingtools.com/**
- **http://www.eblaster.com/**

Fadilla Mutiarawati

Mouse, yang Sering Terabaikan

Mouse sering sekali diabaikan. Umumnya pembeli hanya memilih jenis mouse ketimbang melihat lebih jauh kecepatan dan sensitivitas mous itu sendiri. Padahal dua hal ini sangat mempengaruhi ketepatan mouse. Nilai yang dicari oleh pelaku desainer dan para *gamer*.

Mouse dengan trackball di atas.

Ada saat akan membeli komputer rakitan di sebuah pertokoan, yang tertera sebagai spesifikasi umumnya adalah jenis dan kecepatan processor, RAM, harddisk, serta VGA. Untuk alat input seperti keyboard atau mouse tidak pernah ada keterangan detail kecuali hanya jenisnya saja. Khusus untuk mouse, keterangan yang tersedia terbatas hanya kata-kata "optical", "wireless", "wireless optical", ataupun hanya dituliskan "mouse" saja. Sehingga banyak sekali pembeli yang cenderung tidak terlalu ambil pusing mengenai perangkat yang satu ini. Beberapa yang memiliki kebutuhan tinggi terhadap perangkat pointer ini akan memilih yang paling nyaman digunakan. Misalnya membeli yang wireless atau optical.

Orang-orang ini biasanya adalah mereka yang berkecimpung di bidang desain, seperti desainer grafis, arsitek, dan hampir semua yang mengunakan perangkat lunak *image processor.* Namun, belakangan mouse juga telah menjadi kebutuhan yang sangat diperhitungkan oleh para *gamer*. Karena saat ini permainan-permainan dalam komputer semakin membutuhkan kecepatan dan ketepatan yang tinggi.

Saat ini opsi yang diberikan pedagang di Indonesia umumnya memang hanya ada empat macam saja, yaitu mouse biasa (menggunakan bola yang biasa disebut *trackball*), mouse optical, mouse biasa wireless (tanpa kabel), dan yang terakhir adalah mouse optical wireless.

Dari ke empat jenis yang dikatakan tadi yang kini paling banyak diminati adalah mouse optical dan mouse wireless optical. Kedua mouse ini banyak dipilih karena para pengguna mengira tidak akan lagi membutuhkan mouse pada sebagai landasan mouse yang biasa dipakai oleh mouse biasa.

Jarang ada pembeli yang menanyakan tentang kecepatan dan nilai ketepatan (presisi) sebuah mouse. Mereka cenderung tidak menyadari bahwa dua parameter ini akan menjadi hal yang sangat penting pada pemanfaatan mouse itu sendri. Khususnya untuk kebutuhan-kebutuhan tertentu. Kedua hal ini jugalah yang kadang menjadi penentu harga jual, selain sistem yang digunakannya.

Selain keempat mouse yang disebutkan tadi, masih ada beberapa mouse dengan sistem yang berbeda maupun cara menggunaan yang berbeda seperti laser mouse, trackball, tablet, dan sebagainya. Pointer-pointer ini memang bukan pointer yang lazim digunakan oleh mayoritas pengguna computer di Indonesia. Oleh sebab itu, untuk membeli pointer atau mouse-mouse jenis ini Anda harus langsung bertanya pada si penjual. Karena jarang juga penjual yang memilikinya.

Mouse yang Pertama

Mouse kali pertama diperkenalkan oleh **Douglas Engelbart** pada tahun 1967. Kali pertama diperkenalkannya, mouse hanya memiliki dua alat mekanik berbentuk roda sebagai menanda arah yang masing-masing mengacu pada sumbu X dan sumbu Y. Mouse ini hanya memiliki satu tombol saja pada bagian atasnya. Dan bentuknya masih terlihat sangat primitif. Namun biar demikian, mouse inilah yang telah menjadi cikal-bakal mouse yang kini Anda pergunakan. Untuk dapat memfungsikan mouse sebagai alat penunjuk atau input tidak hanya dibutuhkan fisiknya saja, melainkan juga dibutuhkan keterlibatan software dari mouse itu sendiri.

Perkembangan *software* yang mengirim kemajuan *hardware* dari mouse ini telah mendorong mouse ke posisi yang sangat penting. Baik sebagai *input device* pada pekerjaan sederhana seperti mengetik, sampai pada proses design dan bermain game 3D yang supercanggih.

Mekanik

Mouse yang masih menggunakan bola di bawahnya sebagai alat penggerak pointer di layar monitor adalah mouse yang paling murah saat ini dan sudah disebut mouse saja. Mouse ini harganya paling murah. Dengan uang Rp10.000 saja Anda sudah dapat membeli mouse jenis ini.

Mouse trackball yang tidak menggunakan kabel atau *wireless* hanya membutuhkan tenaga 5 mA saja. Sangat kecil, sehingga Anda tidak perlu sering ganti baterai. Hal ini dikarenakan kerjanya tidak sepenuhnya elektrik. Ada beberapa komponen yang bekerja mekanik, sehingga tidak membutuhkan banyak tenaga listrik. Perawatannya

juga tidak sulit, cukup dibersihkan saja roda-roda mouse, maka mouse dapat berjalan baik kembali.

Pengunaan bola atau yang disebut trackball ternyata tidak selalu di bawah mouse. Saat ini, ada beberapa mouse yang menggunaka bolanya di atas mouse sehingga menggunakannya tidak perlu menelungkupkan telapak tangan. Sehingga lebih mudah dan nyaman digunakan ketimbang mouse biasa. Oleh sebab itu, harganya umumnya lebih mahal dan tidak terlalu banyak perusahaan IT yang memproduksinya. Beberapa di antaranya adalah Microsoft dan Logitech.

Bola yang digunakan untuk mouse jenis ini agak sedikit berbeda. Umumnya lebih besar dan licin. Berbeda dengan mouse yang meletakan bolanya di bawah. Bola tersebut cenderung kecil dengan permukaan yang tidak licin. Hal ini dilakukan agar bola dapat berjalan dengan baik atau tidak tergelincir pada permukaan. Oleh sebab itu, untuk menggunakan mouse mekanik dengan bola di bawah seseorang kerap kali harus menggunakan tatakan khusus yang dinamakan mousepad.

Cara kerja mouse mekanik yang meletakkan trackballnya di atas sama dengan kerja mekanik mouse yang memiliki trackball-nya di bawah.

Optic

Yang disebut mouse optical adalah mouse yang menggunakan sensor cahaya serta lampu LED merah di bawahnya sebagai pencahaya. Sensor pada mouse optical mampu menangkap gambar dengan kecepatan 1500 frame per detik sampai 7000 frame per detik. Dengan kecepatan mencapai 45 inci per detik dengan resolusi 2000 count per inci (cpi).

Mouse ini dinyatakan memiliki nilai presisi yang lebih baik ketimbang mouse yang menggunakan mekanik. Pernyataan ini tidak sepenuhnya benar. Untuk kelas yang sama, mouse optical tidaklah lebih presisi. Yang memang memiliki nilai presisi yang tinggi harganya saat ini masih terbilang mahal. Sedangkan, mouse optical yang umum dijual tidak memiliki kecepatan dan nilai presisi yang lebih baik ketimbang mouse biasa. Dan keterangan ini sering diabaikan oleh si produsen. Coba saja Anda perhatikan boks mouse yang Anda beli, pernahkah ada keterangan kecepatan dan tingkat sensitivitas mouse? Hanya sedikit sekali yang meletakkan keterangan-keterangan itu. Dan umumnya yang meletakkan keterangan-keterangan tersebut adalah mouse-mouse produksi perusahaan-perusahaan besar.

Berbeda dengan mouse trackball yang sulit jalan ditempat yang terlalu licin. Oleh sebab itu, mouse ini membutuhkan sebuah landasannya sendiri yang dinamakan mouse pad. Berbeda dengan mouse optical yang cenderung lebih baik bekerja dipermukaan yang mulus dan dengan warna yang cenderung gelap. Mouse optical sulit dijalankan pada permukaan yang putih polos.

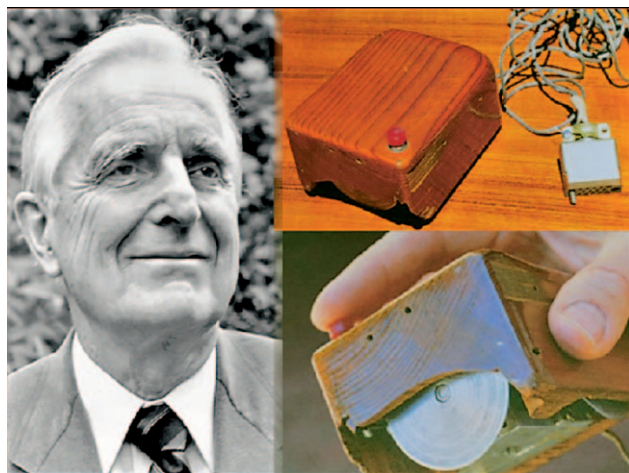
Berbeda dengan mouse mekanik yang sulit jalan di tempat yang terlalu licin, mouse optical dapat digunakan hampir pada seluruh jenis permukaan. Asalkan permukaan tersebut tidak transparan atau terlalu *glossy*.

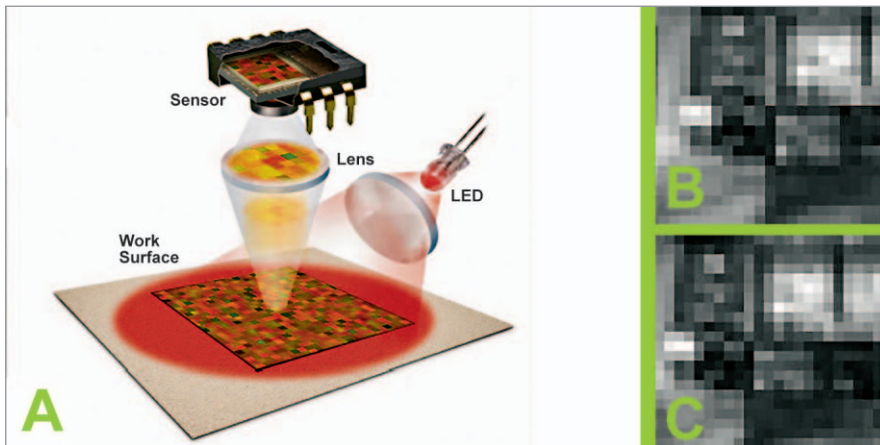
Mouse optic juga membutuhkan arus yang lebih besar ketimbang mouse bola atau mekanis biasa. Lima kali lebih besar arus yang dibutuhkan untuk menggerakan mouse ini (25 mA). Ini artinya bila Anda menggunakan mouse wireless optical Anda akan lima kali lebih sering mengganti baterai ketimbang menggunakan mouse mekanik yang menggunakan bola.

Cara kerja mouse optical adalah sebagai berikut: lampu LED menembarkan cahayanya pada permukaan lalu, sensor cahaya yang ada pada bagian bawah mouse akan menangkap pergeseran yang terjadi pada cahaya tersebut. Atau dapat juga dikatakan sebagai berikut. Bila mouse mekanik komputer mencatat pergeseran yang dilakukan oleh mouse, sebaliknya dengan mouse optical, komputer mencatat pergeseran yang terjadi pada landasan mouse.

Untuk lebih jelasnya perhatikan pada gambar. Bagaimana sebuah sensor mampu menangkap setiap kali adanya perubahan gambar atau pola. Berkaitan dengan pola, hal inilah yang menyebabkan kenapa mouse optical sulit mendeteksi permukaan yang transparan dan glossy seperti kaca atau papan *whiteboard*.

Mouse Laser

Perkembangan mouse optical kini sudah jauh lebih murah ketimbang waktukali pertama diperkenalkannya. Perlahan-lahan kehadiran mouse optical sudah dinilai sangat umum. Kini ada satu mouse lagi yang mulai diperkenalkan kepada masyarakat. Kerjanya hampir sama dengan mouse optical hanya saja bila pada mouse optical biasa menggunakan lampu LED, maka pada mouse laser, bukan lagi sinar LED yang digunakan, melainkan sinar laser. Hal ini membuat ketajaman gam-

Douglas Engelbart dengan mouse ciptaannya.

MX1000 yang menggunakan teknologi laser dari Logitech.

Mouse dengan teknologi optical. Gambar B dan C memperlihatkan bagaimana perubahan pola ditangkap oleh sensor cahaya pada mouse dan diterjemahkan sebagai pergerakan.

bar yang ditangkap oleh sensor menjadi lebih baik. Jika pada permukaan glossy seperti papan whiteboard mouse optical dengan lampu LED-nya sulit membedakan setiap tampilan permukaan, sebaliknya dengan laser, permukaan tidak lagi menjadi sama, melainkan berstruktur atau berpola.

Mouse ini kali pertama diperkenalkan tahun 2004 oleh Logitech yang bekerja sama dengan Agilent Technologies dalam pengembangannya. Teknologi baru ini diklaim mampu memiliki ketepatan 20x kali lebih baik dari mouse optical. Hanya saja harga laser mouse sampai saat ini masih tergolong sangat mahal. Kini, selain Logitech, Microsoft juga ikut meluncurkan mouse berbasiskan teknologi laser ini.

Single Click dan Scroll

Dari sejak awal diperkenalkan, fungsi mouse tidak hanya sebagai penunjuk arah saja. Tetapi, juga sudah berfungsi sebagai input device. Oleh sebab itu, mouse sejak pertama kali diperkenalkan sudah memiliki sebuah tombol.

Waktu kali pertama, memang hanya ada satu tombol yang melengkapinya. Namun kini seiring majunya teknologi pada mouse, tidak hanya tombol saja yang bertambah pada mouse, ada beberapa hal lain yang kini juga telah melengkapi mouse. Di antaranya *scroll button* atau tombol scroll, efek getar, dan masih banyak lagi. Bahkan dari segi keamanan kini juga sudah banyak mouse yang dilengkapi dengan sidk jari.

Tombol yang ada pada mouse memiliki berbagai macam fungsi. Untuk fungsi yang paling umum biasanya terletak pada tombol di sebelah kiri. Sedangkan, untuk fungsi tambahan biasanya terletak disebelah kanan. Scroll mouse banyak dipergunakan untuk melihat sebuah dokumen yang panjang, ke bawah. Sedangkan tombol yang lebih banyak dari itu umumnya sangat terasa manfaatnya bila sedang digunakan untuk bermain *games*. Misalnya saja untuk mengganti senjata, untuk melihat peta, dan sebagainya. Sedangkan pada kebutuhan sehari-hari tombol-tombol tersebut dapat saja diatur untuk memenuhi kebutuhan lain.

Mouse pada aplikasi permainan memiliki fungsi yang tidak jauh berbeda dengan joystick. Kadang sama seperti halnya joystick yang dilengkapi dengan efek getar.

Tidak hanya fasilitas yang beragam bentuk mouse juga sangat beragam. Mulai dari yang sangat kecil (setengah besar telur ayam negeri) sampai sangat besar genggaman telapak tangan. Bahkan ada juga yang berbentuk sangat mirip menyerupai joystick. Sebenarnya apapun bentuk mouse harus disesuaikan dengan kenyamanan penggunanya. Untuk presentasi banyak sekali para pebisnis yang menggunakan trackball wireless yang bentuknya sangat nyaman dalam genggaman seperti layaknya sebuah *remote* atau joystick.

Pilihan Lain

Sebenarnya komputer Anda tidak selalu harus menggunakan mouse. Masih banyak perangkat lain yang dapat beralih fungsi menjadi mouse atau dapat dimanfaatkan sebagai mouse selain fungsi yang lain.

Contoh saja keypad. Dengan bantuan keypad Anda tetap dapat membaca isi sebuah web dengan baik. Dan bila ada isian yang harus dilakukan, Anda dapat mengganti tombol kiri mouse dengan tombol Tab.

Jika ingin lebih mudah lagi, Anda dapat menginstal sebuah program khusus yang dapat menggantikan mouse Anda. Program ini memungkinkan Anda memanfaatkan keyboard Anda tidak hanya untuk mengetik saja, tetapi juga sebagai mouse komputer. Dengan menggunakan keypad-keypad tertentu yang sudah diatur terlebih dahulu. Atau satu lagi alternatif yang dapat digunakan pengguna PC, yaitu Tablet. Sebuah tablet memiliki fungsi seperti mouse lengkap dengan mouse pad khusus, sebuah tablet selalu menggunakan mouse atau *stylus wireless*.

Tablet banyak juga digunakan oleh para desainer. Dan umumnya mereka menggambar menggunakan pensil stylus yang menghadap kepada mousepad itu sendiri. Bentuk stylus pada tablet memang menyerupai stylus pada PDA, hanya saja ada stylus pada tablet umumya memiliki beberapa tombol. Desainer senang menggunakan tablet karena nilai presisi dan kecepatannya yang umumnya lebih baik dari mouse biasa. Oleh karena itu, harga sebuah tablet tidaklah murah seperti halnya mouse biasa.

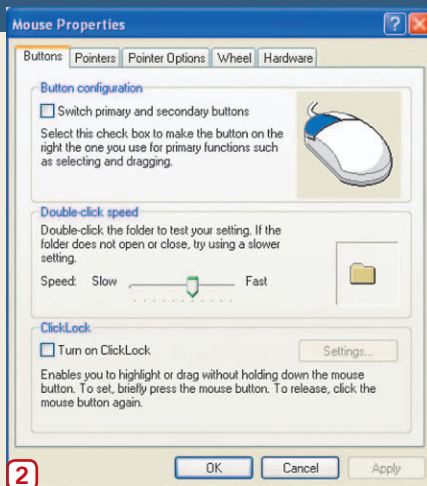
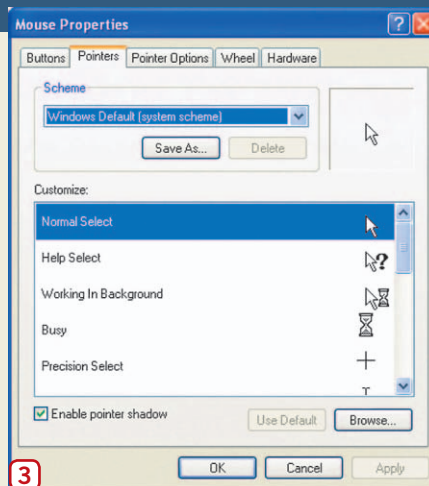
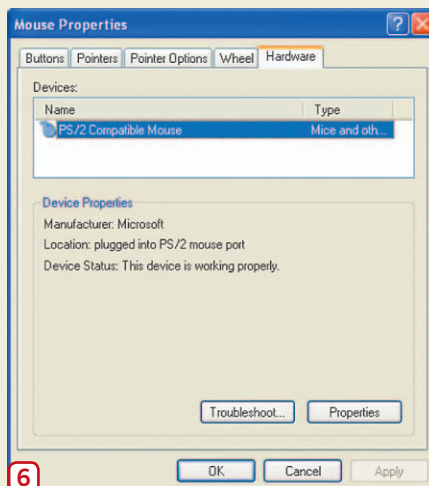
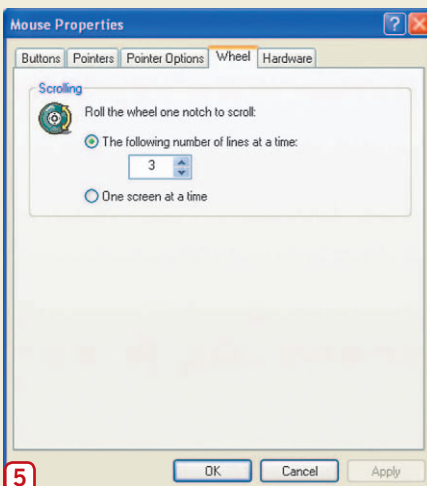
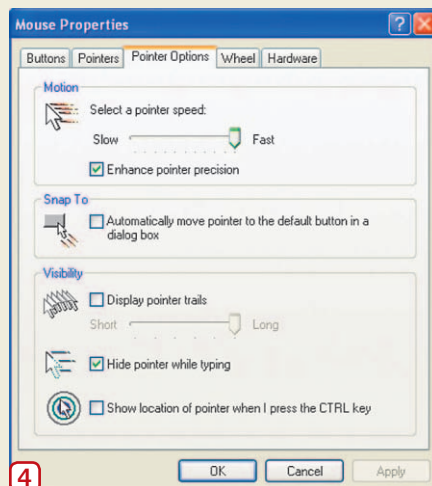
Sedangkan bagi yang menggunakan notebook atau laptop, Anda akan memiliki pilihan yang lebih luas. Karena umumnya sebuah laptop atau notebook sudah dilengkapi dengan alat penunjuk pengganti mouse yang disebut touchpad atau disebut juga *pointer stick*. Jika touchpad bentuknya seperti mousepad kecil dan letaknya di bawah keyboard, pointer stick bentuknya seperti tombol bulat kecil, letaknya di tengah-tengah keyboard.

Pointer stick sangat umum terdapat pada laptop-laptop produksi IBM. Namun, bukan berarti kehadiran mouse akan percuma

Kerja mouse mekanik yang ada sekarang.

Mengatur Atribut Pointer

Anda dapat mengganti tampilan dari pointer yang ada dalam komputer. Mulai dari memberikan bentuk yang berbeda pada masing-masing aktivitas mouse sampai dengan mengatur kecepatan dan buntut yang ada pada pointer Anda.

1. Bukalah *Control Panel*, lalu klik ganda pada icon *Mouse*. Setelah itu *Mouse Properties* akan terbuka.
2. Kemudian bukalah halaman pertama (*Buttons*). Halaman ini mengatur atribut yang berkaitan dengan tombol pada mouse. Dari penentuan fungsi tombol kanan dan kiri, penentuan kecepatan klik ganda sampai penentuan *clickLock*.
3. Halaman kedua digunakan untuk mengatur gambar pointer. Bentuk pointer atau icon apa yang ingin Anda gunakan, silakan pilih dari table *Customize* yang ada di bawah. Jika akan memilih gambar tertentu tekan tombol *Browse*.
4. Halaman ketiga atau *Pointer Option* berguna untuk mengatur kecepatan dan buntut yang ingin ditampilkan pada pointer, serta berbagai atribut lainnya.
5. Halaman keempat digunakan untuk mengatur gerakan *scroll wheel* atau *scroll button*. Roda kecil yang biasanya ada di bagian atas mouse.
6. Dan halaman yang teakhir atau halaman *hardware* digunakan untuk menentukan mouse yang digunakan.

untuk notebook. Mouse atau tablet terkadang masih dibutuhkan pada laptop atau notebook karena kebutuhaannya. Sebab jika terlalu lama menggunakan pointer stick atau touchpad dapat membuat tangan Anda lebih cepat pegal dibandingkan dengan menggunakan mouse biasa.

Meskipun hal ini bukan berarti menggunakan mouse tidak akan berdampak apa-apa bagi kesehatan. Penggunaan mouse yang tidak nyaman dapat membuat pergelangan tangan mengalami penderitaan yang cukup lama. Apalagi bila ukuran mouse memang tidak sesuai dengan kenyamanan tangan Anda. Misalnya saja anak-anak yang menggunakan mouse besar.

Tempat sandaran tangan juga dapat ikut dipertimbangkan. Sekarang ini sudah banyak toko komputer yang menjual sandaran tangan untuk mouse. Bahkan ada juga mouse pad yang memang sudah dilengkapi dengan bantalan khusus. Bantalan ini umumnya terbuat dari bahan *silicon gel* atau *neoprene*. Dan bentuknya sangat bervariasi ada yang menyerupai bantalan biasa, namun ada juga yang berbentuk binatang. Harganya pun bervariasi mulai dari Rp10.000 sampai Rp50.000.

Jenis yang mana pilihan Anda? Terserah saja, mana yang Anda rasakan lebih nyaman. Meskipun mouse yang Anda gunakan memiliki hanya satu tombol, tetapi bila Anda merasa nyaman menggunakannya, maka mouse itulah yang harus dibeli. ■

Lebih Lanjut

- **www.agilent.com**
- **www.logitech.com**

Fadilla Mutiarawati

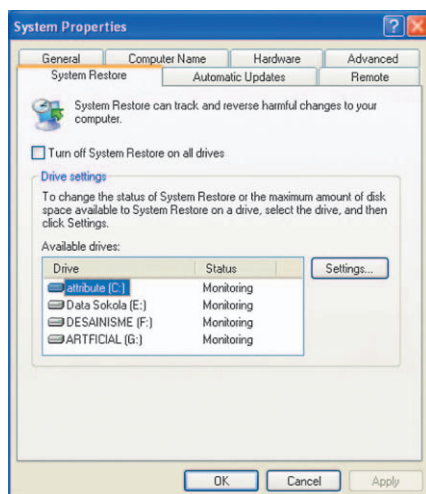
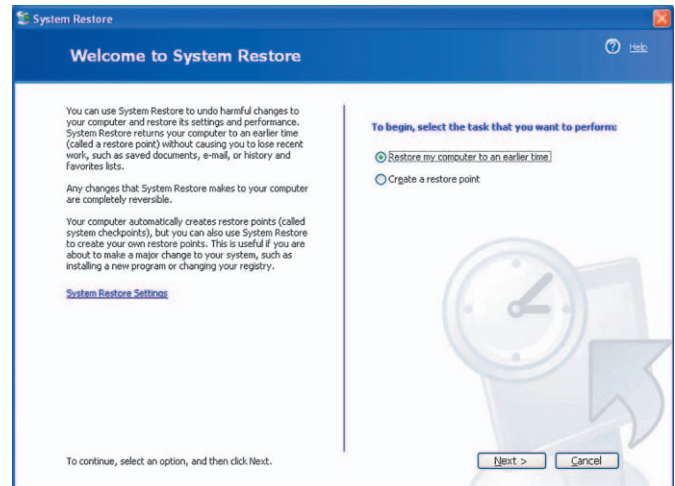
Mengenal System Restore

Berbeda dengan *back-up system restore* hanya mempengaruhi sistem komputer Anda saja, selebihnya tidak. System restore sangat dapat menjadi jalan alternatif ketika sistem pada komputer bermasalah.

Gambar 1.

System Restore bukan fitur baru dalam Windows XP. Bukan juga fitur yang sangat lama. System Restore sudah mulai diperkenalkan sejak Windows Me diluncurkan.

System Restore memungkinkan seorang adiministrator untuk mengembalikan system pada kondisi sebelumnya tanpa kehilangan data personal. Tindakan ini biasanya dilakukan bila perubahan yang diberikan/terjadi pada sistem membuat sistem menjadi tidak stabil atau menjadi tidak sebagaimana mestinya.

System restore memperhatikan setiap perubahan yang terjadi pada system. Dan selalu memberikan tanda pada saat perubahan terjadi. Sehingga Anda dapat mengetahui kapan saja perubahan pada sistem Anda terjadi. Selain mencatat perubahan sistem, system restore juga melakukan pencatatan sendiri yang dinamakan restore checkpoint.

Restore checkpoint adalah titik di mana pemeriksaan dilakukan oleh komputer. Atau dapat juga dikatakan titik waktu di mana komputer melakukan *capture* terhadap system.

Anda dapat mengembalikan kondisi system pada kondisi-kondisi sebelumnya di mana komputer memiliki catatannya. Catatan dilakukan sampai tingkat ketelitian detik. Restore point juga dapat Anda lakukan secara manual dengan dilengkapi keterangan tersendiri.

System restore tidak hanya melakukan restorasi terhadap partisi harddisk yang digunakan untuk *operating system* saja, melainkan semua partisi harddisk. Sebab biasa saja Anda menginstal sebuah program pada partisi yang berbeda dengan letak operating system Anda.

Pembahasan selanjutnya mengenai System Restore hanya akan terbatas pada Windows XP saja.

Gambar 2.

Aktivasi System Restore

Bagaimana mengaktifkan system restore?

Sebenarnya secara standar, system restore akan aktif dengan otomatis, segera setelah Windows berhasil diinstal. Aktifnya system restore membutuhkan minimal 200 MB pada setiap partisi. Jika ruang yang ada tidak mencukupi, maka secara otomatis pula system restore akan dinonaktifkan, sampai kapasitas ruang kembali mencukupi.

Bagaimana bila ingin mengontrol (mengaktifkan atau mematikan) system restore?

Proses kontrol ini dapat dilakukan secara manual, bila Anda inginkan. Caranya ikuti langkah berikut:

1. Klik kanan pada *My Computer*, lalu pilih *Properties*.
2. Pada jendela *Properties*, pilih halaman *System Restore*.
3. Pada halaman ini, Anda dapat mematikan semua system restore pada partisi dengan memberikan tanda centang (✓) pada opsi *Turn off system restore on all drives* (di bagian paling atas). Atau secara manual mematikan system restore satu per satu pada masing-masing partisi. Caranya:
   a. Pilih partisi yang ada di kolom *Available drives*. Lalu tekan tombol *Settings* di sebelah kanan (Gambar 1).
   b. Kemudian berikan tanda centang (✓) pada opsi *turn off System Resore on this drive.*
   c. Sebagai catatan: pada partisi di mana Windows diinstal hal ini tidak dapat dilakukan. Satu-satunya cara mematikan partisi ini adalah dengan mengikuti langkah ketiga di mana system restore pada semua partisi ikut dimatikan.

Dapatkah kapasitas system restore dikecilkan?

Dikecilkan tidak mungkin. Namun bisa diperpesar tergantung pada besar harddisk yang digunakan. Maksimal sampai 12% kapasitas

harddisk. Jika catatan yang dimiliki oleh system restore terus bertambah, maka secara otomatis system restore akan menghapus catatan terlama, ketika ada catatan terbaru akan masuk.

Bila ingin mengatur ruang untuk system restore Anda dapat melakukannya pada System Restore setting yang ada dalam Properties My Computer (perhatikan pertanyaan kedua). Berikut langkah detailnya:

1. Pilih partisi (dalam kolom Available drives) yang akan Anda tentukan kapasitas system restore-nya.
2. Kemudian tekan tombol Setting. Setelah itu tentukan persentase kapasitas yang diinginkan (Gambar 6).

Apakah kerja system restore dapat mempengaruhi kinerja sistem komputer itu sendiri?

Tidak. System restore tidak berkerja non-*stop* secara terus menerus. Ia hanya membutuhkan waktu beebrapa detik saja untuk dapat melakukan pencatatan (*system snapshot*). Dan pencatatan ini juga dilakukan hanya pada saat komputer dalam keadaan menyala, namun tidak sedang digunakan (*idle*).

Siapa saja yang dapat menggunakan sytem restore?

Hanya user yang memiliki hak administrator saja yang dapat melakukan restorasi sistem. Juga untuk melakukan pengaturan sistem restore (pertanyaan kedua dan ketiga).

Meskipun demikian pencatatan restore point yang dilakukan secara otomatis oleh komputer akan tetap berjalan, dengan menggunakan hak *login* siapa saja.

Hanya Sistem Saja

Apa saja yang direstorasi oleh oleh system restore?

Yang direstorasi oleh system restore hanya sistem dan file sistem saja. Selebihnya tidak. Berbeda dengan fitur *back-up* yang menyimpan data personal.

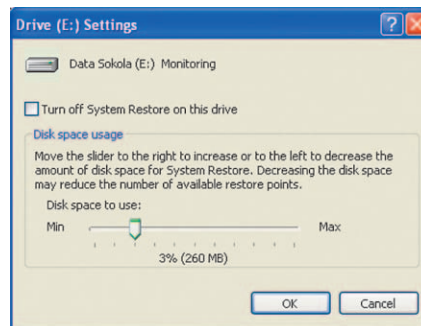
Meskipun demikian, bukan berarti sistem anda kembali menjadi nol atau ter-*reset*. Misalnya saja *password* pada Windows yang tidak akan ikut terrestorasi. Begitu pula password yang ada pada cache memory Internet Explorer Anda.

Namun, lain halnya dengan password yang ada pada program-program. Misalnya password untuk login ke Yahoo!. Umumnya Anda yang mengaktifkan fitur *remember user name and password* atau *automatically login,* tidak akan dapat melihat password Anda masih tertulis di sana, kolom password ini akan kosong.

Jangan panik. Karena password pada aplikasi semacam ini umumnya disimpan pada server di luar komputer Anda, sehingga Anda tidak perlu kawatir. Cukup masukan login dan password yang sama, Anda pun dapat mengakses kembali Yahoo! Messenger Anda.

Apa lagi yang direstorasi dan yang tidak direstorasi oleh system restore?

Berikut adalah data lain yang direstorasi oleh system restore:

- Perubahan yang ada dalam registry
- Profil local)
- COM+ DB
- WFP.dll cache
- WMI DB
- IIS Metabase

Gambar 3.

Dan berikut adalah data lain yang tidak direstorasi dengan system restore:

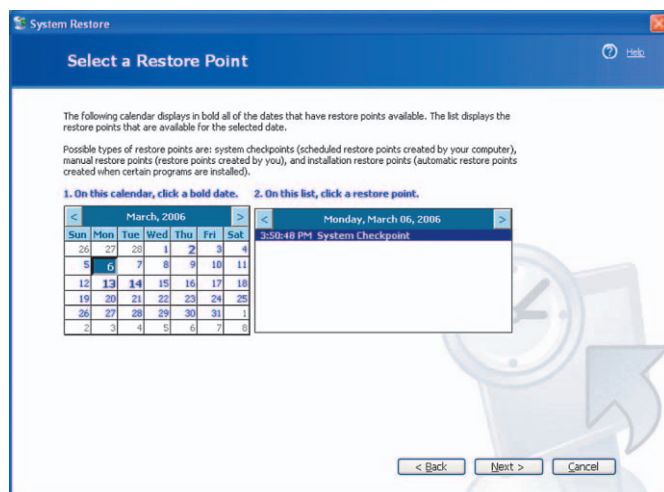
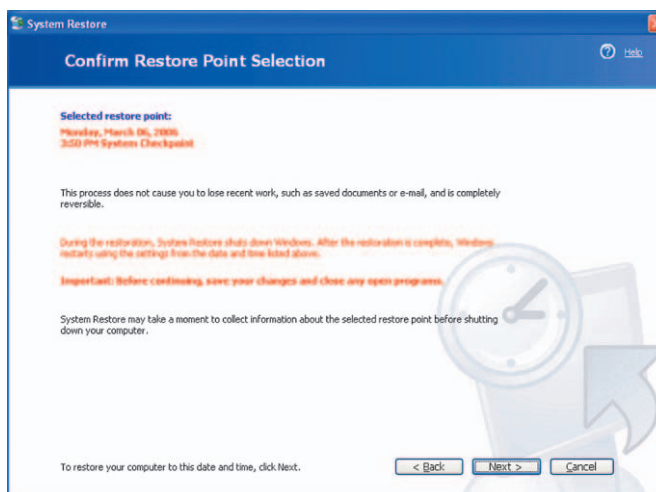
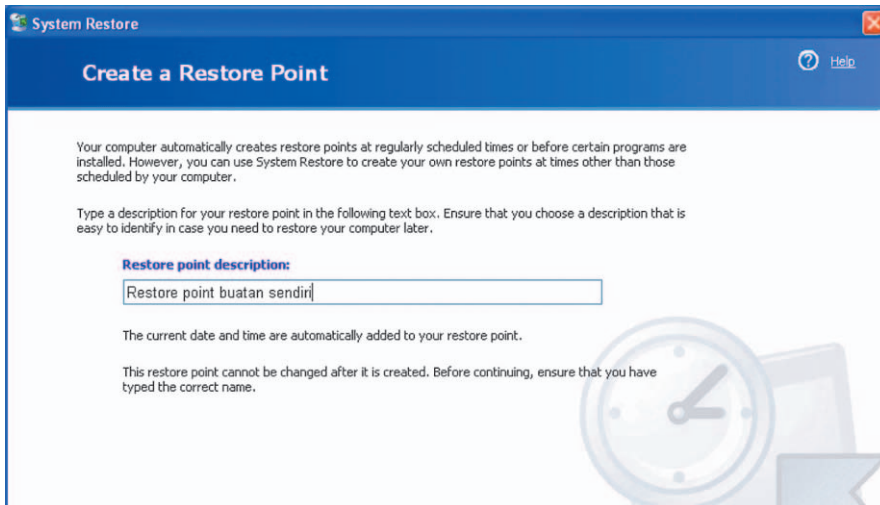
- Setting pada DRM
- Seting pada WPA
- Data pada folder redirect program

Bagaimana dengan aplikasi? Apakah system restore akan melakukan uninstall pada aplikasi tersebut?

Aplikasi yang sudah diinstal tidak akan di-*uninstall* oleh system restore. Apalagi jika aplikasi tersebut memang tidak dimonitor oleh system restore. Oleh sebab itu, ada baiknya bila Anda meng-uninstall terlebih dahulu aplikasi yang akan dihilangkan, kemudian lakukan system restore.

Pada aplikasi, system restore hanya akan menghilangkan perubahan-perubahan baik yang terjadi pada sistem karena aplikasi tersebut maupun pada registry. Serta menghapus semua file tambahan yang berkaitan dengan apliaksi tersebut.

Ingatlah bahwa system restore berbeda dengan back-up

Untuk data personal baik yang tersimpan

Gambar 4.

Gambar 5.

Gambar 6.

Gambar 7.

dalam My document setiap profil atau data pada partisi terpisah, tidak akan mengalami perubahan apapun. Karena memang system restore tidak mengamati file-file seperti itu (.doc, .jpeg, dan seterusnya).

Restore Point

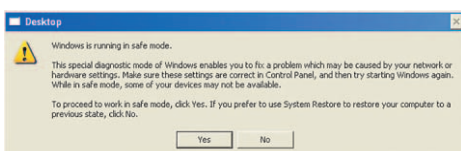
Pada saat kapan saja restore point dilakukan?

Tidak ada waktu pasti kapan restore point dilakukan. Yang pasti pembuatan restore point yang dilakukan secara otomatis oleh komputer hanya dilakukan bila komputer idle. Dan untuk proses ini komputer akan selalu *standby*. Sehingga kapan saja (setiap hari sekalipun) komputer idle, system restore baru membuat *restore point.*

Untuk restore point yang dilakukan dengan cara manual, Anda dapat melakukannya kapan saja diinginkan.

Bagaimana membuat restore point?

Cara membuat restore point secara manual adalah sebagai berikut:

1. Tekan menu Start.
2. Pilih All Programs, Accessories, System Tools, System Restore.
3. Setelah System Restore Wizard terbuka, berikan tanda pada Create a restore point, dan tekan tombol Next (Gambar 2).
4. Berikan nama pada restore point yang Anda buat, tekan Next (Gambar 5).

Gambar 8.

5. Kemudian tekan tombol create (Gambar 5). Restore point yang Anda buat akan dicatat sebagai restore point pada jam dan waktu pembuatan dilakukan.

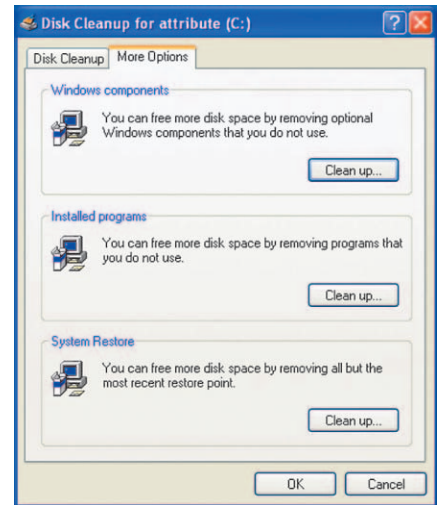
Bagaimana menghapus restore point?

Penghapusan restore point hanya dapat dilakukan sekaligus untuk semua restore point kecuali restore point yang paling terakhir dilakukan. Kecuali Anda menonaktifkan system restore –penonaktifan akan membuat restore point hilang semuanya. Klik kanan partisi di mana restore point ingin dihapus, lalu pilih *Properties*. Kemudian tekan tombol Disk Cleanup dan buka halaman More Option. Setelah itu pada bagian System Restore tekan tombol Clean Up… (Gambar 7).

Bagaimana menjalankan system restore?

System restore dapat digunakan baik dalam modul normal atau Safe Mode. Untuk mengakses system restore dari modul normal:

1. Pilih menu Start, All Programs, Accessories, System Tools, System Restore.
2. Setelah itu pada opsi di kanan atas pilih Restore my computer to an earlier time. Tekan Next (Gambar 2).
3. Tentukan waktu di mana system ingin dikembalikan (Gambar 3).
4. Jika sudah yakin tekan terus Next (Gambar 4), sampai kemudian system restore akan berjalan.
5. Setelah selesai menjalankan restorasi akan muncul layar memberikan laporan.

Untuk menjalankan system restore pada halaman safe mode, Anda dapat langsung menekan opsi tersebut pada saat akan masuk dalam Safe Mode. System restore dalam safe mode sangat berguna bila ternyata kerusakan yang ada membuat Anda tidak dapat melakukan booting sebagaimana normalnya. Sehingga dapat kembali dengan mudah ke keadaan sebelum booting gagal.

Bagaimana? Sekarang Anda sudahmengetahui apa manfaat system restore. Tidak ada salahnya lagi menggunakan system restore ini dari pada harus berkali-kali menggunakan opsi *repair* atau perbaikan yang ada pada Windows. Proses system restore hanya makan waktu sebentar. Setelah system restore dijalankan, komputer akan me-*restart* dan login dalam modul biasa. Bila sudah seperti ini, maka komputer sudah dapat digunakan kembali.

Sedangkan proses selanjutnya adalah sama. Untuk lebih lanjut mengenai Safe Mode baca saja artikel khusus tentang safe mode yang ada dalam edisi ini.

Catatan:

Setiap kali selesai menyingkirkan sebuah virus, sebaiknya Anda mereset system restore Anda. Agar pada saat system restore dijalankan, virus tidak tersimpan atau terinstal kembali. Cara me-reset system restore adalah dengan cara menonaktifkan sementara lalu mengaktifkannya kembali dengan segera.

Hal ini dikarenakan untuk virus-virus tertentu, mereka akan kembali terrestorasi begitu system restore dijalankan. Oleh sebab itu, harus benar-benar diperhatikan ketika Anda terfikir untuk menjalankan system restore. ■

Fadilla Mutiarawati

Manfaat Safe Mode

Dengan masuk dalam *safe mode*, Anda banyak memperbaiki komputer yang terluka, baik karena virus atau karena aplikasi yang tidak benar. Bahkan bila ada kerusakan driver yang membuat Anda tidak dapat *booting* dengan benar dapat diperbaiki dalam safe mode.

"Lakukan dalam safe mode!" Kata-kata ini kerap muncul pada saat komputer terserang virus-virus kebal yang sulit dibasmi. Seakan-akan dalam safe mode virus akan kehilangan kekebalannya. Apa benar demikian?

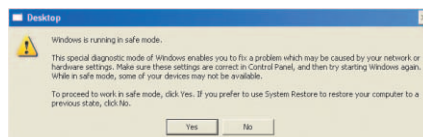
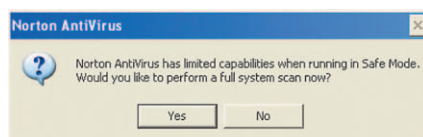
Ya. Dalam safe mode *operating system* akan berjalan secara minimalis dan semua aplikasi akan ditidurkan, sehingga dalam safe mode sangat efektif membasmi virus.

Lebih dari itu safe mode ternyata memiliki fungsi yang lebih dalam lagi. Tidak hanya berkaitan dengan virus dan kawan-kawanya saja. Dalam safe mode, Anda dapat melakukan banyak perbaikan yang biasa dilakukan para teknisi komputer.

Oleh sebab itu dengan mempelajari safe mode lebih jauh, Anda dapat menghemat biaya perbaikan komputer yang biasa dilakukan oleh teknisi-teknisi di Mangga Dua.

Masuk dalam safe mode bukanlah langkah yang sulit. Pertama-tama nyalakan komputer atau *restart* komputer, lalu setelah selesai loading RAM, tekan F8. Dalam Windows XP, Anda akan diberikan beberapa pilihan untuk modul safe mode. Yang pertama *Safe Mode with Networking, Safe Mode with Command Prompt,* dan yang terakhir *Safe Mode* saja. Bila Anda ingin dapat terhubung ke jaringan tempat komputer terhubung atau ingin menggunakan koneksi Internet ketika berada dalam safe mode, maka pilihlah pilihan yang pertama. Bila akan menggunakan safe mode dalam bentuk command promt seperti layaknya DOS atau Linux, gunakan Safe Mode with Command Prompt. Namun bila hanya ingin menggunakan Safe Mode biasa tnpa terhubung dengan jaringan apapun, pilih saja Safe Mode.

Jika Anda penggunakan Windows XP Pro, maka dapat memilih login yang akan digunakan asalkan memiliki izin sebagai admin. Sedangkan, para pengguna Windows XP Home hanya ada login administrator yang ditwarkan dengan password yang dikosongkan. Sehingga hanya seseorang yang mengetahui password administrator utama saja yang dapat masuk dalam safe mode Windows XP Home.

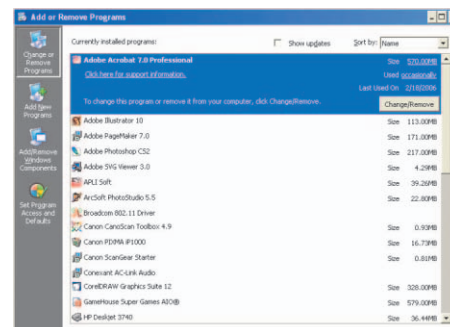
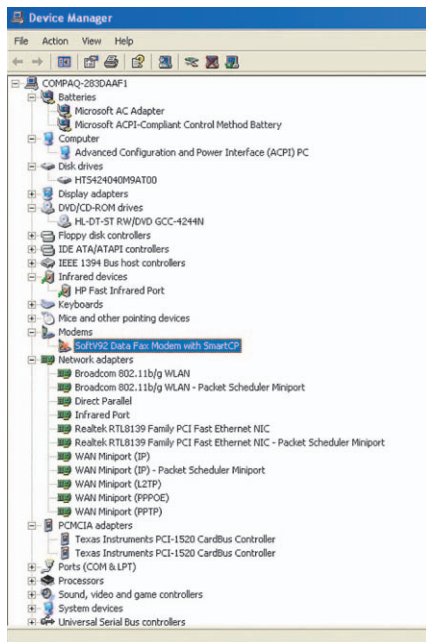
Ketika akan masuk dalam safe mode, Anda akan ditanyakan apakah yakin atau tidak. Jika ya, maka lanjutkan. Jika tidak lebih baik mundur. Meskipun sebenarnya tidak akan berbahaya masuk dalam safe mode. Masuk dalam safe mode sama saja dengan login sebagai administrator. Tidak ada yang berbeda, selain keminimalisan operating system, perangkat keras, dan tidak aktifnya aplikasi (perangkat lunak).

Menghilangkan Virus dalam Safe Mode

Pada awal wacana sempat dikatakan bahwa pembasmian virus dan kawan-kawannya sering menjadi agenda utama seseorang masuk dalam safe mode. Mungkin sebagian Anda sudah banyak yang mengetahui bagaimana menghapus virus dalam modul biasa. Bagaimana dalam safe mode? Lebih mudah. Karena dalam safe mode tidak banyak pengaturan yang harus dilakukan. Sebagian besar aplikasi antivirus ternama pada modul safe mode akan otomatis melakukan pemeriksaan secara menyeluruh (Gambar 3). Oleh sebab itu, melakukan *scanning* pada safe mode memang cenderung lebih lama.

Selain virus yang sulit dibasmi, dalam safe mode Anda juga dapat menghapus *adware* dan *spyware*. Caranya sama saja. Jalankan program anti spyware dan anti adware, scan seperti halnya men-scan virus dengan antivirus. Maka, spyware dan adware pun dapat hilang seperti layaknya virus.

Mengapa dengan safe mode bisa, sedangkan tanpa safe mode tidak? Karena pada umumnya aplikasi perusak sekali mendapat izin untuk aktif, maka ia akan terus menginstal dirinya sendiri setiap kali di hapus atau di-*uninstall*. Bahkan ada beberapa aplikasi adware atau spyware yang pada saat aktif memang tidak dapat dihentikan atau dihapus. Dalam safe mode semua aplikasi ini tertidur, sehingga dapat dimatikan. Dalam modul biasa aplikasi pengganggu umumnya akan aktif pada saat komputer mulai dinyalakan.

Mengakses System Restore

System restore adalah salah satu fitur yang sangat efektif untuk mengembalikan system Anda pada keadaan di mana kerusakan atau konflik sistem belum terjadi. Misalnya pemasangan driver yang salah atau adanya perangkat yang tidak kompatibel dengan

Gambar 1.

Gambar 3.

Gambar 2.

Gambar 4.

Windows XP. Dengan system restore, Anda dapat mudah mengembalikan kondisi komputer kembali ke waktu di mana perangkat tersebut belum diinstal.

System restore dapat diakses melalui menu *System Tools*, dalam modul normal. Namun adakalanya di mana kerusakan atau ketidakcocokan alat/driver mengakibatkan user sulit memasuki modul normal atau dapat disebut juga komputer gagal booting. Oleh sebab itu, salah satu jalan keluarnya adalah dengan mengakses system restore dari modul safe mode.

Bahkan setiap kali akan memasuki modul safe mode, Anda akan selalu ditanya oleh komputer apakah akan bekerja dalam safe mode atau hanya akan menjalankan system restore. Jika Anda ingin menjalankan system restore, pada sat awal memasuki safe mode pilih saja No (lihat Gambar 1).

Kemudian Anda dapat menajlankan system restore sebagaimana layaknya menjalankan system restore pada modul normal. Semua langkah dalam menggunakan system restore tidak ada yang berbeda, baik dalam safe mode maupun dalam modul normal. Untuk lebih jelas mengenai safe mode, bagaimana menggunakannya dan bagaimana mengaturnya, Anda dapat membaca artikel khusus tentang safe mode pada edisi ini.

Memperbaiki Komputer Rusak

Komputer yang tidak dapat dipergunakan ada banyak sebabnya. Mulai dari aplikasi yang rusak sampai pada kerusakan fisik. Beberapa kerusakan ini sebenarnya dapat dengan mudah diperbaiki dalam safe mode, ketimbang harus dibawa ke tempat servis yang tidak jarang membutuhkan waktu dan biaya yang besar. Beberapa petunjuk di bawah ini nantinya dapat Anda pergunakan untuk memperbaiki beberapa kerusakan komputer dengan safe mode. Namun, terlebih dahulu Anda harus mengenali jenis kerusakan apa yang dialami komputer Anda.

Cara mengetahuinya adalah dengan mengidentifikasi di mana kegagalan terjadi. Jika komputer gagal menjalani proses booting, pada saat sedang *loading* Windows atau kemudian diam dan layar menjadi biru, maka kekacauan *dating* dari driver atau hardware yang tidak cocok.

Sedangkan bila yang terjadi adalah system *crash* pada saat proses loading selesai dijalankan, atau pada saat Windows sedang melakukan proses *start up,* maka yang menjadi biang keladinya adalah aplikasi yang aktif pada saat start up. Baik karena proses instaliasi yang tidak sempurna, karena konfliknya aplikasi dengan aplikasi lain, atau hardware yang ada. Semuanya bisa saja menjadi penyebab.

Kerusakan Software

Kerusakan yang ditimbulkan oleh aplikasi cukup beragam, di antaranya adalah aplikasi tersebut dapat membuat system mengalami crash baik pada saat komputer selesai loading antar muka atau pada saat aplikasi dijalankan. Bahkan ada juga beberapa aplikasi atau service yang membuat system sepenuhnya gagal booting.

Masalah-masalah yang ditimbulkan oleh aplikasi ini sebenarnya memiliki banyak solusi sebelum akhirnya diselesaikan dengan safe mode.

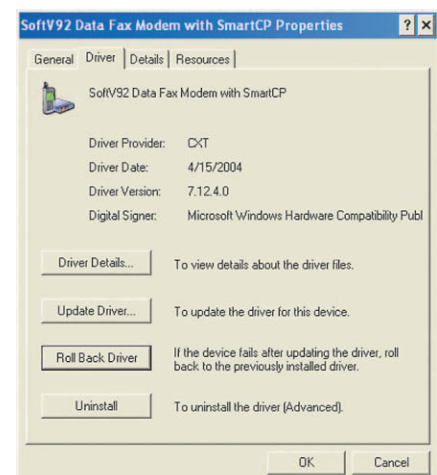
Yang pertama adalah dengan meng-uninstall aplikasi melalui control panel, Add/Remove Programs (Gambar 2). Lalu install ulang. Yang kedua adalah dengan menjalankan system restore. Jika keduanya berhasil, maka tidak perlu masuk dalam safe mode. Namun jika keduanya tidak dapat dilakukan, atau setiap kali akan melakukan keduanya komputer mengalami crash, karena konflik yang terjadi antara aplikasi dengan hardware. Maka langkah selanjutnya barulah menggunakan safe mode. Langkah menggunakan safe mode juga akan dengan sendirinya harus Anda lakukan bila kerusakan membuat Anda sulit masuk dalam antarmuka Windows XP yang normal. Umumnya ditimbulkan oleh aplikasi yang aktif pada saat start up.

Langkah awal adalah masuk dalam safe mode. Kemudian lakukan proses uninstall dari safe mode. Cara ini umumnya sangat efektif. Karena kemungkinan system mengalami konflik sangat minim.

Jika tidak mengetahui program apa saja yang jalan pada saat start up, maka Anda dapat menggunakan bantuan aplikasi khusus (yang dapat mendeteksi *auto run* aplkasi)atau dengan dengan menggunakan perintah 'msconfig'. Caranya tekan Start, Run, lalu pada box Open isi msconfig, kemudian tekan OK.

Setelah itu buka halaman Startup. Pada halaman ini Anda dapat menandakan mana saja aplikasi yang ingin Anda pilih untuk tetap diaktifkan dan mana yang tidak (Gambar 6). Lalu tekan tombol Apply. Lalu jalankan kembali Windows dalam modul biasa.

Namun jika tidak diketahui aplikasi mana yang mengacau, Anda perlu menjalankan trik sebagai berikut:

- Jalankan 'msconfig' dalam safe mode lalu pilih bagian startup. Dan langsung tekan tombol Disable all. Tekan tombol Apply lalu booting komputer dalam modul biasa.
- Kemudian dalam modul biasa, jalankan kembali 'msconfig', dan buka kembali bagian startup.
- Setelah itu, pilihlah satu persatu aplikasi untuk diaktifkan. Setiap kali menaktifkan satu aplikasi, booting kembali komputer.

Gambar 5.

- Lalukan terus sampai Anda mengalami crash atau masalah yang biasa muncul. Dengan begitu, Anda dapat mengetahui sebenarnya palikasi mana yang jadi gara-gara.
- Bila sudah diketahui, lakukan proses penonaktifan aplikasi tersebut atau uninstall secara langsung aplikasi dalam safe mode.

Gambar 6.

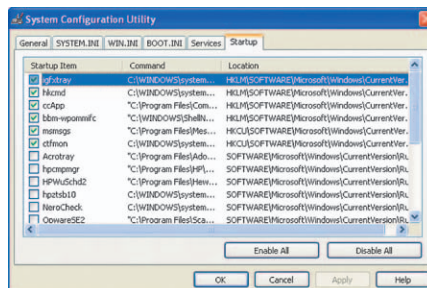
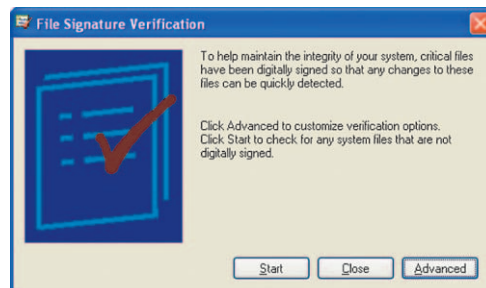
Gambar 7.

Kerusakan Hardware

Jika Anda salah meng-update driver, dengan mudah Anda dapat menjalankan Roll Back Driver. Namun, kadang untuk menjalankan roll back driver tidak sesederhana itu. Sebab bila ternyata terjadi konflik, maka akan ada kemungkinan system crash dan tidak mau booting ke dalam modul normal sehingga proses roll back driver harus dilakukan dalam safe mode.

Proses roll back driver (Gambar 5) dapat dilakukan jika memang Anda mengetahui driver mana yang bermasalah. Namun, hal ini tidak berlaku bila Anda tidak mengetahui driver mana yang bermasalah.

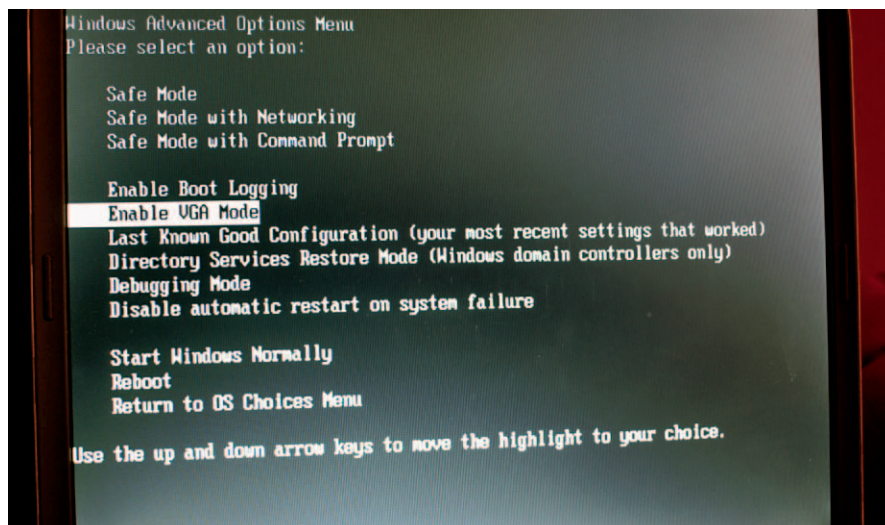
Umumnya permasalah driver bila tidak karena salah driver-nya, maka kesalahan lain adalah driver yang rusak atau tidak dapat diterima oleh operating system. Dalam Windows XP, Anda boleh mencurigai driver-driver yang tidak memiliki sertifikasi Windows XP. Cara mengetahui driver mana saja yang tidak memiliki sertifikasi Windows XP adalah dengan menjalankan perintah 'sigverif' (pilih Start menu, Run, tuliskan 'sigverif' lalu tekan OK) (Gambar 7).

Namun, belum tentu semua driver ini bermasalah dengan operating system Anda. Oleh sebab itu, Anda harus mengetesnya satu per satu. Sebelum mengetes, sebaiknya Anda jalankan 'sigserif' tersebut dalam modul safe mode. Lalu—setelah Anda mengetahui driver mana saja yang bukan bersertifikasi Windows—cut dan paste file tersebut dari c:\windows\system32\drivers\ ke dalam folder yang Anda buat sendiri (misalnya diberikan nama backup driver).

Kemudian kembalikan (dengan cut dan paste) satu per satu driver ke dalam folder c:\windows\system32\drivers\ satu per satu sambil me-reboot komputer dalam modul biasa—pada setiap satu file dipindahkan—sampai Anda mengalami masalah atau sampai komputer tidak mau reboot atau crash. Dengan begitu, Anda akan mengetahui driver mana yang bermasalah. Cut dan paste driver tersebut kembali ke folder yang Anda buat sebelumnya. Lalu cari penggantinya yang lebih baik. Bila sudah dapat instal kembali driver.

Namun, jangan lakukan hal ini pada driver VGA. Untuk driver VGA caranya cukup dengan roll back driver atau update driver. Dan mengakses menu driver VGA dalam safe mode adalah sebagai berikut. Setelah jalankan safe mode, klik kanan pada desktop, lalu pilih Properties. Kemudian itu pilih halaman Setting, tekan tombol Advance di bagian bawahnya. Lalu pada halaman adapter tekan tombol Properties. Pada halaman driver Anda dapat melakukan tindakan-tindakan yang disebutkan tadi.

Bila ada perangkat yang setelah dipasang justru membuat komputer crash atau menolak booting, maka Anda harus men-*disable*-kan (menonaktifkan) terlebih dahulu perangkat tersebut dalam modul safe mode (Gambar 4). Kemudian cari driver yang benar kemudian instal driver tersebut dalam modul normal. Setelah terinstal dengan benar, barulah *enable*-kan kembali perangkat Anda dalam modul normal juga.

Tidak jarang juga berkaitan dengan VGA, adalah nilai *refresh rate* yang tidak sesuai dengan kemampuan monitor, sehingga kadang monitor tidak mau menampilkan antarmuka operating system-nya dengan baik. Cara memperbaikinya tekan tombol F8 (seperti akan masuk dalam safe mode) namun jangan pilih Safe Mode, melainkan pilih 'Enable VGA Mode'. Dengan begini komputer akan me-reset pengaturan VGA pada nilai standar, yaitu resolusi 640x480 dengan refresh rate 60 Hz. Untuk mengubahnya tekan menu Start, Control Panel, Display, Settings, Advance. Kemudian Dalam halaman Adator tekan tombol 'list all modes'. Cobalah opsi yang Anda inginkan, bila tidak ada keganjilan, berarti cocok. Jika sudah cocok, reboot kembali komputer dalam modul normal.

Banyak bukan yang dapat Anda lakukan dengan Safe mode? Tidak perlu lagi terburu-buru ke tukang servis. Lain kali cobalah dulu Anda perbaiki sendiri. ■

Gambar 8.

Lebih Lanjut

- www.microsoft.com

Gunung Sarjono

Keyboard, Bahaya dan Pembersihannya

Hati-hati pada waktu makan sambil mengetik. Apakah itu sarapan, makan siang, *snack*, serpihan dan potongannya bisa masuk ke dalam keyboard. Mari kita lihat makanan yang aman buat keyboard, bersama dengan cara membersihkannya.

Kita semua melakukannya, meskipun kita tahu bahwa itu tidak boleh. Apakah itu makan *snack* untuk membantu menghabiskan waktu atau makan siang sambil mengembalikan file kerja yang tidak sengaja terhapus, kita semua makan di tempat keyboard. Pada suatu hari, keyboard terkena cipratan kopi, saus mie, dan bahkan serat yang jatuh dari pisang

Pada waktu membersihkannya, kita akan tahu bahwa mereka adalah makanan yang berbahaya pada waku dimakan sambil mengetik. Hal ini bisa dilihat dari tiga faktor, yaitu kecenderungan makanan untuk jatuh, kemungkinan makanan menempel atau masuk ke dalam keyboard, dan tingkat kesulitan dalam membersihkan. Dengan mengacu ketiga faktor tersebut, berikut adalah makanan yang bisa membahayakan keyboard.

Nasi

Makanan ini mudah dan kemungkinan masuk ke dalam keyboard, tetapi membersihkannya relatif mudah jika dibiarkan kering dulu sebelum itu dilakukan.

Pasta

Meskipun kemungkinan tidak jatuh, pasta bisa meninggalkan bekas. Jika bekas pasta ternyata bercampur dengan saus maka itu bisa menempel pada tombol, atau bahkan jatuh di antara mereka. Membersihkan mereka tidak sulit kecuali jika pasta benar-benar tidak terlihat. Jika demikian, maka pembersihan hampir tidak mungkin dilakukan. Jika salah satu ujungnya menonjol, pegang pelan-pelan dengan telunjuk dan jempol lalu tarik perlahan-lahan. Cara ini bisa memberikan manfaat tambahan karena sekaligus mengangkat fragmen kecil yang secara tidak sengaja menempel pada pasta.

Kwaci

Tidak mungkin kita makan lebih dari 12 biji kwaci tanpa menjatuhkan satu pun potongan di bawah tombol, meskipun itu bergantung kepada cara makan yang dilakukan. Begitu masuk ke dalam keyboard, kwaci terkenal sulit untuk dibersihkan, karena membalikkan keyboard biasanya tidak lebih dari memindahkan potongan tersebut dari dasar keyboard ke dalam rongga tombol.

Rice Krispies (dengan atau Tanpa Susu)

Rice krispies kering bisa ke manapun. Satu tiupan angin pelan dan mereka akan ada di rambut Anda, dan masuk ke daerah keyboard. Namun, menghilangkan mereka relatif mudah; tekan tombol berulang-ulang selama beberapa menit untuk menghancurkan mereka menjadi serpihan dan kemudian lakukan penyedotan. Rice Krispies basah lebih stabil tetapi lebih sulit dicabut. Meskipun Krispies basah tersebut telah mengering, mereka cenderung sulit dicabut karena menempel erat ke bagian dalam keyboard.

Jell-O

Jell-O sifatnya tidak stabil dan cepat terpisah pada waktu digerakkan. Begitu jatuh ke keyboard, Jell-O cenderung bersitahan pada keyboard dan turun di antara mereka, terutama jika Jell-O banyak mengandung air. Membersihkan Jell-O merupakan pekerjaan yang sulit dan kotor dan kadang-kadang menyebabkan tombol tidak seperti dulu lagi. Jell-O bebas gula yang dua per tiganya mengandung air cenderung memantul daripada menempel.

Cadbury Flake

Bagi yang belum tahu, ini adalah batang coklat yang dibuat dari lapisan coklat yang sangat tipis yang dilipat-lipat beberapa kali. Memakan *flake* dekat keyboard adalah hal yang sangat berbahaya. Tidak mungkin menggigit flake tanpa menyebabkan jatuhnya butiran-butiran kecil. Meskipun butiran coklat tidak mengganggu pengetikan atau menyebabkan suara keyboard yang aneh, flake tetap menjadi salah satu makanan yang berbahaya bila dekat keyboard. Flake hanya boleh dimakan pada waktu santai, di atas kertas tisu untuk menampung remah-remah, atau dalam mangkok besar. Jika Anda harus makan flake dekat keyboard, yang cukup dimengerti, coba ganti dengan makanan yang kurang berbahaya.

Membersihkan Tumpahan Komputer

Sains tidak bisa menjelaskannya, tetapi minuman ringan dan kopi tidak disangkal lagi tertarik dengan keyboard komputer. Jika diletakkan berdekatan, maka cepat atau lambat mereka akan merusak keyboard. Untuk membersihkan tumpahan keyboard:

2. Jika Anda menumpahkan air, balikkan keyboard dan biarkan mengering selama paling sedikit 24 jam.
3. Jika Anda menumpahkan cairan yang lengket, coba lepaskan tombol keyboard yang kecil dengan obeng minus supaya bisa lebih leluasa. Jangan cabut tombol spasi, tombol Enter atau tombol yang besar. (Foto layout keyboard atau buatlah sketsanya sebelum mencabut tombol supaya Anda bisa memasangnya kembali dengan benar.)
4. Perlahan-lahan bersihkan keyboard dengan kain lap katun basah.
5. Pasang tombol setelah membilas mereka dan mengeringkannya.
6. Biarkan semuanya mengering paling sedikit 24 jam sebelum memasang keyboard kembali.

Membersihkan Tumpahan ke Laptop

Menumpahkan kopi ke laptop tidak hanya akan mengacaukan pagi Anda, tetapi juga bisa mengacaukan komputer Anda. Cepatlah bertindak jika ini terjadi, karena cairan hanya butuh beberapa detik untuk meng-

Membersihkan Keyboard Komputer

■ Tampilan yang kotor hanyalah salah satu alasan untuk membersihkan keyboard komputer. Jika debu masuk ke bawah tombol, mereka tidak bisa bekerja dengan baik. Dan cairan yang tumpah juga bisa mematikan keyboard jika tidak ditangani. Untuk melakukannya:

1. Beli perangkat yang Anda perlukan: udara kempaan (dalam botol aerosol); kain lap lembut; cairan pembersih yang cocok untuk membersihkan plastik; dan masker debu jika Anda alergi terhadap debu.
2. Baca manual Anda. Jika pabrikan menyediakan instruksi khusus, ikuti mereka.
3. Matikan komputer.
4. Cabut keyboard.
5. Gunakan udara kempaan untuk membersihkan ruang antara tombol. Semprot pada sudut tertentu untuk mengeluarkan debu dan kotoran.
6. Balik dan goyangkan keyboard perlahan-lahan untuk menjatuhkan debu dan kotoran.
7. Jika menggunakan cairan pembersih, ikuti instruksi pabrikan. Atau, semprotkan sedikit ke kain lap.
8. Bersihkan tombol dan casis keyboard.
9. Tunggu sampai keyboard kering sebelum memasangnya kembali ke komputer.
10. Pasang keyboard dan nyalakan komputer.

Tip Membersihkan keyboard

■ Udara kempaan adalah teman Anda – bisa untuk menghilangkan partikel kering dari keyboard. Pilihan lain, gunakan vacuum cleaner untuk mendapatkan hasil yang sama, tetapi pastikan tombol-tombol keyboard terpasang dengan baik. Tentu tidak menyenangkan jika Anda harus membuka-buka penampung kotoran/debu untuk mencari tombol yang copot.

Mungkin terdengar aneh, beberapa orang menggunakan mesin pencuci piring untuk membersihkan keyboard secara menyeluruh. Jika Anda membersihkan keyboard dengan mesin pencuci piring, bilas keyboard dengan air suling sebelum mengeringkannya selama paling sedikit 72 jam. Bergantung pada air di tempat Anda, banyak mineral yang bisa menyebabkan masalah kelistrikan. Lebih baik aman daripada menyesal, terutama jika Anda mempunyai keyboard multimedia yang mahal, meskipun mampu membeli yang baru. Kunjungi link pada kotak lebih lanjut untuk mendapatkan informasi lebih lengkap tentang bagaimana cara melakukannya.

Tombol kotor bisa dihilangkan dengan pembersih layar. Matikan komputer terlebih dulu (menekan tombol berulang-ulang pada waktu membersihkan bisa menimbulkan hasil yang tidak diinginkan). Masing-masing bisa dicopot dan digosok dengan air sabun hangat untuk mendapatkan hasil pembersihan yang lebih menyeluruh. Untuk lingkungan kotor atau berdebu, tidak ada salahnya untuk membeli tutup keyboard meskipun bisa mengurangi kenyamanan pada waktu mengetik.

Jika Anda menumpahkan banyak cairan, atau jika cairan lengket maka kemungkinan besar keyboard tidak akan bisa diperbaiki meskipun Anda mencobanya. Paling aman adalah meletakkan minuman sejauh mungkin dari komputer Anda. Keyboard tidak begitu mahal. Jika Anda menumpahkan banyak sekali cairan, akan lebih mudah membeli yang baru daripada membersihkannya.

Jika Anda sering bekerja dengan beberapa laptop, selalu letakkan minuman di bawah laptop. Jangan coba untuk meletakkan minuman pada meja yang sama dengan laptop. Jauhkan minuman teman dari laptop pada waktu bekerja satu meja. Itu uang Anda jadi lindungilah.

Peringatan

Jika Anda menumpahkan cairan ke keyboard, cabut dan balikkan keyboard supaya cairan keluar. Jika banyak cairan yang masuk, atau jika cairan lengket, semprot dengan air (jangan celupkan keyboard). Biarkan keyboard kering selama 72 jam. Jangan semprotkan cairan langsung ke keyboard. Jangan cabut satu tombol pun dari laptop kecuali jika manual menyediakan cara untuk melakukannya.

Membersihkan Keyboard Laptop

Cara membersihkan dan cairan yang sesuai bisa mengembalikan keyboard laptop Anda seperti baru. Ada beberapa hal yang menyebabkan tombol macet, yaitu cairan yang tumpah, penggunaan cairan yang tidak sesuai standar pabrikan, mengerasnya bantalan karet yang digunakan, dan kontaminasi oleh debu dan rambut. Untuk mengatasi masalah tersebut dan mengembalikan kondisi keyboard Anda harus menyiapkan dulu kain lap katun, karet busa pembersih kosmetik (hanya gunakan dengan nafta (cairan pemantik), jangan alkohol), tisu, alkohol, air, nafta (cairan pemantik), penjepit lancip, gunting, saringan dapur, pembersih rumah atau sejenis, semprotan Super Lube Dry Film – ini merupakan cairan PFTE (teflon) yang kering secara sempurna dan cocok digunakan di sini.

Bongkar

Penting: Buat gambar keyboard supaya Anda tahu posisi masing-masing tombol. Secara hati-hati lepaskan setiap tombol dengan obeng minus kecil dan masukkan ke dalam wadah. Mereka akan melompat. Jangan gunakan kekuatan yang berlebihan. Bisa saja ada potongan karet kecil pada setiap tombol. Lepaskan mereka semua dan masukkan ke dalam wadah terpisah. Hati-hati, mereka berukuran kecil dan cenderung sulit terlihat.

Bersihkan Keyboard

Bersihkan keyboad dengan menggunakan kain lap katun yang telah sedikit dibasahi dengan air karena jika terlalu basah maka air bisa masuk ke dalam keyboard. Ini akan membersihkan semua cairan yang dapat larut dengan air seperti Coca-Cola, kopi, dan sisa gula. Untuk tempat yang sangat sempit, potong karet busa menjadi bagian-bagian kecil dan basahi sedikit lalu gunakan penjepit untuk membersihkan. Anda harus membersihkan setiap tombol, luar dan dalam. Ini sangat penting karena inilah tempat tombol bersentuhan dan bergerak.

Ulangi lagi langkah ini dengan menggunakan alkohol dan kain lap katun, tetapi jangan dengan menggunakan karet busa karena bisa hancur jika digunakan bersama alkohol. Terakhir ulangi dengan menggunakan nafta (cairan pemantik) dan karet busa. Ini akan menghilangkan kotoran minyak dan gemuk pada tombol berukuran lebar yang mempunyai kawat, misalnya Space Bar.

Bersihkan Tombol

Beberapa tombol mempunyai kawat yang diolesi dengan gemuk. Bersihkan dulu mereka dengan kain lap katun dan nafta (cairan pemantik). Hilangkan semua bekas gemuk. Masukkan semua tombol ke saringan. Semprot dengan pembersih rumah dan diamkan selama lima menit. Bilas secara seksama dengan air panas dan letakkan tombol di atas tisu supaya mengering. Biarkan sampai benar-benar kering.

Bersihkan Komponen Karet

Masukkan semua komponen karet ke saringan. Tutup saringan supaya mereka tidak hilang jika meloncat. Semprot dengan pembersih rumah dan diamkan selama lima menit. Bilas secara seksama dengan air panas dan letakkan di atas tisu. Lipat tisu dan tekan untuk mengeluarkan air dari karet. Biarkan sampai benar-benar kering.

Lumasi Tombol

Letakan semua bagian atas-bawah tombol di atas tisu. Lapisi tombol dengan cairan Super Lube Dry Film. Lakukan ini dari keempat sisi supaya bisa menjangkau tempat yang kecil. Biarkan mengering. Jangan terlalu lama melakukan langkah ini karena pelarutnya bisa memperngaruhi plastik.

Lumasi Keyboard

Tutupi laptop dengan kertas dan selotip. Semprotkan pelumas ke keyboard dan biarkan mengering. Sekarang Anda sudah membersihkan dan melumasi tombol, keyboard, dan komponen karet.

Pasang Kembali

Masukkan semua komponen karet ke dalam keyboard. Pasang tombol yang menggunakan kawat. Pastikan kawat sudah pas di dalam tombol, biasanya dimasukkan ke suatu tempat. Masukkan ujung kawat satunya ke tempat tombol pada waktu memasangnya. Secara perlahan-lahan tekan untuk memasukkan tombol ke dalam tempatnya. Pasang sisa tombol yang lain dengan cara yang sama. Sekarang keyboard Anda bisa berjalan dengan baik dan lancar.

hancurkan harddisk laptop Anda. Untuk melakukannya:

1. Segera matikan komputer.
2. Bersihkan setiap cairan. Miringkan laptop untuk mengeringkan cairan.
3. Cabut komponen yang bisa dilepaskan dari laptop, termasu kawat power, kabel printer dan mouse, floppy drive, CD drive, modem, dan baterai. Jangan bongkar badan laptop untuk mencabut komponen internal.
4. Setelah komponen dicabut, perlahan-lahan angkat laptop dan balik-balikkan untuk mengeringkan cairan. Miringkan laptop ke berbagai arah untuk memastikan tidak ada cairan yang bersembunyi, tetapi hati-hati untuk tidak menggoyangkan atau menanganinya secara kasar.
5. Lakukanlah hal yang sama untuk floppy drive serta komponen lain yang dilepaskan.
6. Gunakan pengering rambut (pada level cool) untuk mengerinkan laptop dan komponennya jika memungkinkan.
7. Biarkan laptop dan komponen yang dicabut mengering selama 24 jam sebelum Anda memasang dan menyalakannya kembali. (Jika terburu-buru, biarkan laptop mengering paling sedikit satu jam sebelum Anda memasangnya).
8. Jika laptop tidak berfungsi dengan baik atau tidak mau menyala, bawa ke tempat servis meskipun kerusakan mungkin saja tidak bisa diperbaiki. Tumpahan cairan merupakan salah satu yang bisa menyebabkan laptop mati. ■

Lebih Lanjut

- **http://www.kador.com**
- **http://www.rabidhardware.net**

Bernaridho I. Hutabarat

Pendidikan Perangkat Keras

Tulisan pada artikel ini adalah bagian dari serangkaian tulisan tentang cara memajukan penguasaan teknologi informasi di negeri ini. Ada beberapa isu terkait yang berperan pada keberhasilan pendidikan perangkat keras.

Beberapa isu tersebut, antara lain nama jurusan, penyediaan sarana, sifat dan durasi pendidikan, serta kesesuaian penyerapan alumni terhadap materi pendidikan.

Berbagai Istilah untuk Teknologi

Pendirian suatu program pendidikan harus dilandasi visi dan misi. Salah satu masalah yang menghadang dalam pendefinisian visi dan misi adalah banyaknya istilah yang terkait. Saya daftarkan beberapa istilah yang pernah maupun yang masih terkenal: *Information Technology, Electronic Data Processing,* dan *Information Communication Technology*.

Esensi istilah-istilah tersebut sama. Tapi, pemilihan istilah ini saja akan menimbulkan perdebatan. Para personil pendiri atau dosen biasanya berjuang untuk mendapatkan istilah yang "wah dan trendy".

Berbagai Nama Jurusan

Bila masalah istilah telah diselesaikan, masalah lain muncul. Masalah ini adalah pemilihan nama jurusan. Mungkin dari berbagai nama jurusan pendidikan perangkat keras komputer yang ada di Indonesia saat ini, hanya ada tiga jurusan yang dominan. Ketiga jurusan itu mencakup Teknik Elektro, Teknik Komputer, dan Teknik Telekomunikasi.

Apakah nama jurusan berperan dalam keberhasilan pendidikan? Ya. Tidak jarang terjadi bahwa seorang mahasiswa tidak begitu berminat dalam pendidikan karena setelah berada di dalam ia merasa jurusan tersebut tidak seperti apa yang ia bayangkan. Perbedaan antara kenyataan dengan apa yang dibayangkan sedikit banyak dipengaruhi oleh nama jurusan/program studi/spesialisasi.

Penyediaan Perangkat Keras

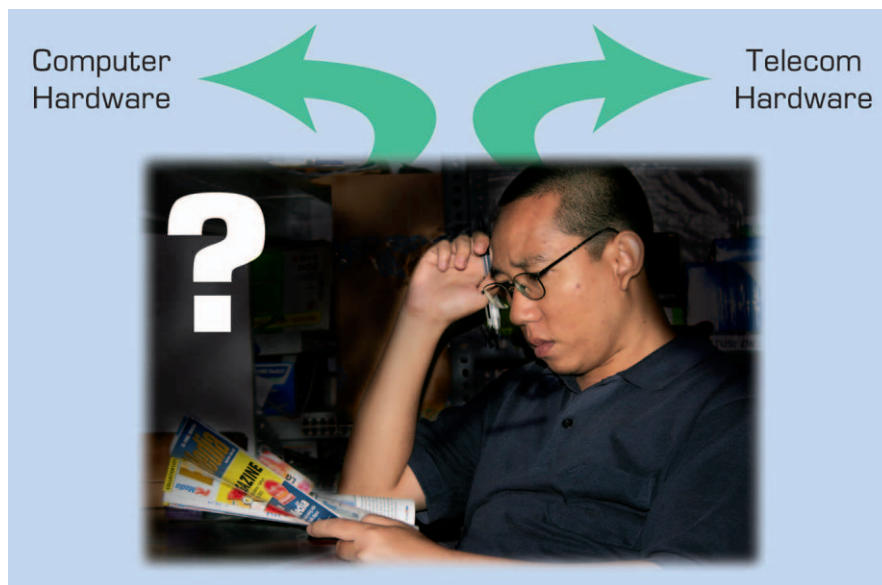
Bila beberapa orang sudah sepakat bahwa jurusan yang mereka kelola berfokus pada perangkat keras komputer, mereka harus menyepakati perangkat keras apa yang menjadi sarana belajar utama. Harga perangkat keras tertentu sangat mahal.

Sebagai contoh, bila jurusan yang ingin dibuat berfokus pada telekomunikasi, maka para pendiri harus memikirkan penyediaan perangkat keras untuk praktikum. Harga perangkat keras *handphone*, switch, router, dan modem masih terjangkau. Tetapi, harga perangkat keras BTS (*Base Transceiver Station*) dan satelit tidak terjangkau. Para pendiri jurusan harus berpikir keras untuk menyediakan alat-alat tersebut dalam praktik. Solusi yang biasa adalah kerja sama dengan operator telekomunikasi.

Bila jurusan yang ingin dibuat berfokus pada perangkat keras komputer, maka para pendiri harus memikirkan penyediaan perangkat keras komputer untuk server dan komputer untuk client. Perangkat keras, seperti handphone, switch, router, dan modem bersifat sekunder. Mereka mungkin perlu praktikum dengan perangkat keras RAID (*Redundant Array of Independent Disks*), SCSI (*Small Computer System Interface*), dan lain-lain. Perangkat keras RAID dan SCSI tidak menjadi fokus jurusan perangkat keras telekomunikasi.

Varian Perangkat dan Efek terhadap Nama

Pada awal dekade 1980 mudah untuk membedakan subjurusan telekomunikasi dengan subjurusan teknik (perangkat keras) komputer. Saat itu tidak ada handphone, PDA (*Personal Digital Assistant*), smartphone, PDA–phone, atau perangkat-perangkat lain dengan nama-nama yang sangat beragam. Saat itu mustahil programer biasa dapat memprogram perangkat telekomunikasi dengan mudah. Memprogram perangkat keras telekomunikasi hanya dapat dilakukan dengan perangkat keras khusus.

Sekarang pembedaan jurusan atau subjurusan itu menjadi lebih rumit. Saya telah mencoba memberi solusi tentang pemakaian

Gambar 1. Apakah fokus ke *computer hardware* atau *telecom* hardware?

Gambar 2. Telecom *hardware* untuk praktikum telekomunikasi.

perangkat keras yang disesuaikan terhadap fokus pendidikan. Tetapi, nama jurusan masih memiliki masalah yang terkait dengan perangkat keras. Apakah namanya "Teknik Perangkat Keras Komputer" dan "Teknik Perangkat Keras Telekomunikasi"?

Apa yang disebut "Komputer" saat ini dalam praktiknya hadir dengan banyak nama. handphone, PDA, smartphone adalah komputer. Perangkat keras dari tipe-tipe di atas dapat diprogram, dan dalam sebagian kasus programnya dapat berupa perangkat lunak yang dapat diubah.

Solusi terhadap masalah nama jurusan adalah tetap memakai kata komputer seperti pada frasa "Teknik Perangkat Keras Komputer". Kekurangjelasan dapat diminimalkan dengan paparan yang baik pada brosur dan *website*.

Perlukah? Kepedulian Akan Industri

Sekarang sebuah pertanyaan yang sangat penting adalah "Perlukah pendidikan perangkat keras komputer dan perangkat keras telekomunikasi?" Dengan cara yang sekarang tidak perlu.

Kata Teknik pada jurusan-jurusan yang sekarang ini kurang tepat dalam menggambarkan esensi pelajaran yang seharusnya diberikan di banyak jurusan. Kata "Rekayasa" (*engineering* dalam bahasa Inggris) lebih tepat. Rekayasa Perangkat Keras Komputer dan Rekayasa Perangkat Keras Telekomunikasi adalah nama-nama jurusan yang lebih tepat untuk menggambarkan isi buku-buku teks yang dipakai.

Tujuan pendidikan dari kedua jurusan tersebut adalah menghasilkan *computer hardware engineer* dan *telecom hardware engineer* (*telecommunication* sering disingkat *telecom*). Anda dapat melihat iklan-iklan perusahaan operator telekomunikasi dan pembuat perangkat keras telekomunikasi yang mencari *network engineer, telecom engineer*, dan *radio* (*network*) *engineer*.

Mengingat esensi pendidikan yang seharusnya, pendiri jurusan-jurusan di atas harus bertanya: apakah ada industri yang menampung lulusannya? Apakah di Indonesia ada industri pembuatan perangkat keras komputer dan industri pembuatan perangkat keras telekomunikasi yang dapat menampung lulusannya untuk menerapkan sebagian besar ilmu di kuliah? Tidak. Bilapun ada pabrik perangkat keras telekomunikasi dan komputer di Indonesia, lulusan sekolah teknik di sini paling hanya menjadi *supervisor, manager, sales engineer*, atau yang lainnya.

Untuk Sekadar Wawasan?

Argumen yang cukup sering diajukan tentang perlunya pendidikan perangkat keras adalah peningkatan wawasan. Alumni dan pelaku pendidikan menganggap bahwa kita tidak harus bekerja sesuai latar belakang pendidikan.

Argumen ini sah untuk level pribadi. Tapi, jumlah uang yang dikeluarkan untuk "menambah wawasan" ini sangat besar pada level nasional, karena jumlah mahasiswa teknik elektro dan teknik telekomunikasi yang cukup besar.

Dalam skala besar seperti ini, biaya dan upaya yang sudah dikeluarkan terlalu besar. Sudah berapa ribu orang mempelajari puluhan buku teks dengan jumlah halaman total mencapai puluhan ribu tapi tidak memberi hasil yang seharusnya? Adalah lebih baik untuk memakai uang dan usaha tersebut ke sesuatu yang lebih produktif.

Jadi, walau secara pribadi alasan menambah wawasan dapat diterima; dalam level nasional alasan ini tidak dapat diterima. Kita secara nasional telah membuang begitu banyak uang, waktu, dan tenaga. Menambah wawasan tentang perangkat keras komputer dan telekomunikasi tidak harus dengan membaca puluhan ribu halaman buku teks, puluhan buku teks, dalam jangka waktu empat tahun, dan dilakukan oleh sangat banyak orang seperti saat ini.

Sebuah Pengalaman Pendidikan di Luar Negeri

Pendidikan level S2 (strata 2) saya pada bidang telekomunikasi, persisnya M. Sc in Operational Telecommunication. Pendidikan berlangsung di Cable & Wireless College, college yang didirikan sebuah perusahaan telekomunikasi internasional yang cukup berpengaruh: Cable & Wireless. Banyak porsi pendidikan membahas perangkat keras telekomunikasi.

Ada hal menarik dari lembaga pendidikan tersebut, yang terkait dengan topik pendidikan perangkat keras. Pertama, adalah tersedianya sarana-sarana perangkat keras yang jarang ditemukan pada saat itu di Indonesia. Mahasiswa angkatan tahun 1995 sudah dapat memakai perangkat keras *mobile phone, fixed phone* untuk *teleconferencing* (dengan jumlah partisipan tiga atau lebih), antena BTS, dan ATM (*Asynchronous Transfer Mode*). Perangkat-perangkat keras ini dipakai untuk penelitian dan pembuktian teori. Apakah ada lembaga pendidikan perangkat keras di sini yang dapat menyediakan perangkat-perangkat keras tersebut dalam keadaaan yang tidak berbeda terlalu jauh dengan keadaan yang *current*?

Perusahaan yang Melakukan Riset

Sebuah perusahaan bernama Qualcomm berperan dalam mewujudkan temuan bernama CDMA (*Code Division Multiple* Access) ke masyarakat. Mungkin Qualcomm bukan perusahaan pertama yang menyelidiki CDMA, dan mungkin Qualcomm juga bukan perusa-

haan pertama yang coba memasarkan CDMA. Tetapi, Qualcomm adalah perusahaan yang berhasil meyakinkan masyarakat industri dan masyarakat pemakai untuk mengembangkan dan memakai teknologi CDMA.

Dalam kasus di Indonesia, masuk akalkah harapan kita akan adanya perusahaan seperti Qualcomm? Bila harapan ini tidak masuk akal, tentunya jumlah jurusan pendidikan perangkat keras telecom dan komputer juga tidak masuk akal. Mayoritas alumni tidak akan menemukan wadah yang tepat yang sesuai dengan pendidikannya.

Nice-to-have dan Persaingan dengan Para Otodidak

Sadar atau tidak, suka atau tidak, pendidikan perangkat keras di negeri ini efektifnya menghasilkan alumni yang secara mayoritas akan menganggap pendidikan tersebut bersifat *nice-to-have*, memberi wawasan. Sebagian kecil alumni berusaha membuat pendidikan tersebut tidak nice-to-have.

Apa wujud usaha mereka ini? Sebagian besar hanya akan menjadi dosen di dalam negeri. Sebagian kecil yang beruntung akan dapat bekerja di luar negeri (baik sebagai dosen maupun praktisi/*engineer*). Sebagian kecil mungkin akan bekerja di industri yang sedikit memanfaatkan ilmu mereka. Bila beruntung, penghasilannya cukup baik; bila tidak, penghasilannya pas-pasan.

Untuk alumni yang tetap menerapkan ilmunya dan bekerja di Indonesia, dan mendapat penghasilan yang pas-pasan; biasanya ada fenomena di internal keluarga. Besar kemungkinan istri/suami akan sering mempertanyakan mengapa dia mempertahankan idealismenya. Istri/suami juga mungkin akan menunjuk bahwa orang yang tidak kuliah saja bisa terjun di industri telekomunikasi dengan menjadi pelaku dan/atau pemilik jasa di bidang telekomunikasi bergerak (reparasi handphone, kolumnis, membuat majalah, menjadi konsultan, penyedia *content*). Hal yang mirip terjadi untuk alumni industri perangkat keras komputer.

Bersaing dengan Alumni Pendidikan Perangkat Lunak

Efek tidak tersedianya pekerjaan yang seharusnya bagi alumni pendidikan perangkat keras adalah masuknya mereka ke pekerjaan yang seharusnya ditempati *software engineer*. Hal ini adalah salah satu sebab sangat banyak alumni pendidikan teknik elektro yang akhirnya menjadi programer atau praktisi teknologi olah data. Kejadian yang mungkin "lebih parah" adalah banyaknya alumni teknik elektro menjadi dosen di jurusan Informatika. Politeknik Informatika Del di Laguboti hanya salah satu contoh. Kebanyakan dosennya justru alumni teknik elektro, bukan teknik informatika.

Engineer dalam Sense Kedua, Sebuah Kompromi?

Mungkin kita bisa berkompromi untuk menyediakan pendidikan perangkat keras yang tepat guna. Dalam hal apa? Dalam hal perangkat keras telekomunikasi, bukan perangkat keras komputer.

Gambar 3. ***Computer hardware*** **untuk praktikum komputer.**

Iklan berbagai operator dan vendor perangkat keras telekomukasi sering mencantumkan frasa *Radio Engineer, Network Engineer,* dan *Telecom Engineer.* Engineer dalam "sense" ini bukan perekayasa, mereka tidak merekayasa perangkat keras. Mereka adalah personil yang sangat mengerti pemakaian perangkat keras.

Mungkin ada perlunya pendidikan perangkat keras untuk menghasilkan personil-personil di atas. Masalahnya berapa lama dan pada strata berapa pendidikan seperti itu? Lamanya maksimal dua tahun, dan strata 2. Pendidikan ini tidak bersifat nice-to-have, tetapi menghasilkan engineer dalam sense kedua di atas.

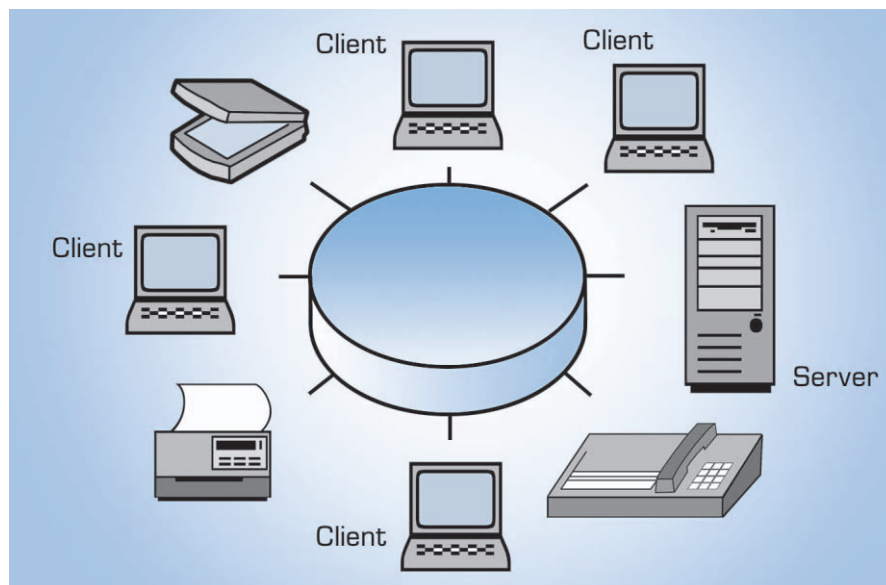
Khusus untuk perangkat keras komputer, lama pendidikan juga maksimal dua tahun, dan strata 2. Pendidikan ini bersifat nice-to-have, tidak menghasilkan engineer. Tahun pertama berkonsentrasi pada perangkat keras, sedangkan tahun kedua pada aspek manajemen teknologi olah data.

Penutup

Jelaslah bahwa secara umum, pendidikan perangkat keras komputer dan telekomunikasi di Indonesia ini masih bersifat sekadar nice-to-have atau "menambah wawasan". Dengan sifat seperti ini, pendidikan perangkat keras komputer dan telekomunikasi sebaiknya didominasi pendidikan pada level S2 karena pendidikan pada level S2 memang biasanya bersifat "menambah wawasan".

Pendidikan level S1 yang bertujuan untuk membangun perekayasa sebaiknya hanya ada pada PT (Perguruan Tinggi) yang berkonsentrasi untuk menghasilkan alumni dengan pasar yang sempit, alumni yang mutunya sangat tinggi untuk menjadi kandidat doktor dalam bidang tersebut. Dengan cara seperti ini, maka pemborosan biaya oleh beberapa pribadi dapat diminimalkan. Ini adalah salah satu langkah awal untuk meningkatkan penguasaan teknologi informasi (olah data) di Indonesia. ■

Lebih Lanjut

- **[Tane1999] Andrew S. Tanenbaum; Structured Computer Organization,4th ed; Prentice Hall**
- **[Tane2003] Andrew S. Tanenbaum; Computer Networks,4th ed; Prentice Hall**

Hayri

Power-over-Ethernet: Perkawinan Listrik dan Data

Bayangkan jika dulu para penemu teknologi jaringan dan komunikasi data sangat menghindari pertemuan antara jalur data dan jalur listrik, kini mereka mengawinkannya menjadi satu.

Dari dulu kerja sama antara sinyal-sinyal listrik dan transportasi data hanya sampai pada batas perangkat saja. Sinyal listrik menghidupkan perangkat jaringan yang akan digunakan untuk mentransfer data. Transportasi data yang sebenarnya juga merupakan sinyal-sinyal listrik tersebut memiliki tugas dan jalurnya sendiri yang tidak bisa diganggu.

Seiring meluasnya penggunaan sistem komunikasi data, perangkat jaringan dan transmisi data juga menemui masalah baru yang berkaitan dengan kebutuhan sumber daya listrik. Contoh, berkembangnya penggunaan *Wireless Access Point*. Perangkat wireless ini harus menjadi sangat fleksibel dalam digunakan. Perangkat ini harus mampu untuk diletakkan di mana saja, dalam kondisi bagaimanapun, juga harus dapat bekerja dengan baik.

Salah satu yang timbul pada perangkat wireless AP ini atau perangkat sejenis lainnya adalah masalah kelistrikkan. Jika Anda meletakkan sebuah AP di atas auning atau di atap-atap ruangan sebuah gedung, tentu akan sangat sulit untuk menyediakan sumber listrik bagi perangkat ini. Anda harus memperpanjang kabel listrik untuk kemudian dapat digunakan oleh adaptornya mensuplai tenaga listrik untuknya. Masalah ini tentu bukanlah masalah sepele karena memang tidak mudah untuk menyediakan sumber listrik di lokasi-lokasi sulit tersebut. Belum lagi adaptor-adaptor yang harus mendukung sumber listrik untuk perangkat ini biasanya cukup besar fisiknya. Tentu akan sangat repot mencari tempat peletakannya.

Berangkat dari masalah ini, para ahli mulai menciptakan teknologi yang dapat menyelesaikan masalah kelistrikkan untuk perangkat jaringan dan elektronik yang berada di lokasi ekstrem tersebut. Atas dasar itulah, terciptalah teknologi *Power over Ethernet* atau PoE.

Teknologi Seperti Apakah PoE?

Power over Ethernet adalah teknologi transportasi tenaga listrik yang digunakan untuk menghantarkan tenaga listrik ke perangkat komputer atau jaringan. Sekilas teknologi ini memang biasa saja, namun ia menjadi sangat luar biasa karena tenaga listrik yang dihantarkan ke perangkat bukanlah seperti yang biasanya terjadi. Penghantaran ini dibuat menjadi berbarengan dengan transmisi datanya. Disebut berbarengan karena memang dilakukan secara bersamaan dan dalam satu media. Jadi dengan demikian teknologi ini akan membawa perubahan besar dalam hal transportasi tenaga listrik ke dalam perangkat jaringan dan komputer yang ada saat ini.

Tenaga listrik dan data dibawa dalam satu buah media yang sama. Media yang biasanya digunakan untuk proses ini adalah kabel UTP (*Unshielded Twisted Pair*) Category 5 atau 5e. Kabel ini sudah sangat familiar di kalangan pengguna jaringan komputer karena kabel jenis inilah yang paling banyak digunakan saat ini dalam jaringan data yang bersifat lokal atau LAN. Jaringan data LAN yang umum digunakan saat ini di perkantoran, perumahan, warnet, dan banyak lagi, biasanya menggunakan teknologi yang bernama Ethernet. Maka dari itu, teknologi transmisi tenaga listrik yang dibarengi dengan jalur data di dalam LAN ini diberi nama *Power over Ethernet.*

Apa Tujuannya Diciptakan PoE?

Hampir semua perangkat komputer dan perangkat komunikasi data yang sekarang ada membutuhkan dua komponen ini, yaitu sumber daya dan media transportasi data. Contoh yang paling familiar adalah perangkat telepon. Perangkat telepon yang saat ini ada di rumah-rumah Anda sebenarnya merupakan konsep dasar teknologi PoE ini. Dalam satu utas kabel tembaga telepon mengalir dua komponen penting, yaitu sinyal-sinyal listrik dan sinyal-sinyal suara yang merupakan komponen utama. Sekarang kita dapat melakukan hal yang sama dengan menggunakan teknologi PoE. Berikut ini beberapa alasan dan tujuan mengapa teknologi PoE diciptakan:

- Hanya dengan seperangkat kabel yang akan menghemat biaya dan juga tempat, Anda dapat mengaktifkan sekaligus menggunakan perangkat komputer dan jaringan data. Proses instalasi menjadi mudah dan sederhana, tidak banyak kabel berkeliaran dan biaya yang terbuang percuma.
- Instalasi perangkat sangat mudah, Anda tidak membutuhkan waktu yang lama dan tidak perlu meminta bantuan ahli listrik untuk memasang steker atau memasang kabel ekstension di dekat perangkat Anda. Tinggal colok saja kabel yang merupakan jalur power ke dalam port yang benar di perangkat Anda.
- Perangkat komputer dan jaringan menjadi lebih fleksibel bergerak selama kabel UTP/ kabel LAN Anda juga bebas bergerak.
- Lebih aman karena tidak ada jalur listrik yang lain kecuali dari kabel tersebut. Meminimalisasi terjadinya kebakaran pada steker atau kabel power.
- UPS dapat digunakan bersama-sama dan lebih mudah dengan menggunakan PoE, tidak perlu memperpanjang kabel listrik untuk koneksi ke UPS. Perangkat menjadi lebih aman dan minimal *downtime*-nya.
- Seperti halnya transportasi data, jalur listrik yang melalui PoE ini juga dapat dimonitor dengan lebih mudah menggunakan protokol monitoring yang biasa digunakan dalam

jalur data, yaitu protokol SNMP.
- Perangkat jaringan dan komputer dapat diaktifkan dan dimatikan secara *remote*, tidak perlu melakukannya secara fisik apalagi jika sulit dilakukan.

Bagaimana Cara Kerja PoE?

Teknologi PoE kali pertama dirancang menjadi sebuah sistem standar oleh organisasi standarisasi IEEE pada tahun 1999. Pemain teknologi ini pada awal terciptanya adalah 3Com, Intel, PowerDsine, Nortel, Mitel, dan National Semiconductor. Kemudian standar ini baru rampung pada 12 Juni 2003 dengan kode standar IEEE 802.3af.

Ada dua jenis teknik penyuntikan sinyal-sinyal listrik DC ke dalam kabel UTP jalur data:

Penyuntikkan melewati kabel-kabel yang "nganggur" atau kabel spare.

Pada intinya, teknologi ini bekerja dengan memanfaatkan kabel-kabel *spare* yang ada pada sistem komunikasi data berbasis teknologi Ethernet dengan menggunakan kabel UTP cat 5. Seperti telah Anda ketahui, kabel UTP yang Anda gunakan untuk komunikasi ethernet (10BaseT) ataupun Fast ethernet (10BaseTX) hanya menggunakan dua pasang atau empat buah inti kabel saja dari seutas kabel UTP. Sedangkan, dalam seutas kabel UTP tersebut terdapat empat pasang atau delapan buah inti kabel.

Dari penggunaan ini terdapat dua pasang kabel yang sangat tidak efektif karena hanya dibiarkan terbentang saja padahal tidak digunakan sama sekali. Atas dasar ini, terciptalah teknologi PoE. PoE membuat keempat inti kabel ini menjadi bermanfaat dan bahkan membawa perubahan cukup besar dalam dunia jaringan komputer. Kedua pasang kabel yang biasa digunakan biasanya adalah kabel nomor 1, 2, 3, dan 6. Keempat buah inti kabel ini akan saling menghubungkan komponen transmit (TX) dan komponen receive (RX) dari masing-masing perangkat yang dihubungkan. Ketika semuanya terhubung, maka proses komunikasi terjadi.

Aplikasi teknologi PoE akan sangat banyak beberapa tahun mendatang.

Keempat buah kabel lainnya yang "nganggur" tadi kemudian dirangkai sedemikian rupa untuk dapat dihubungkan dengan sumber tenaga listrik DC seperti adaptor, baterai, atau power supply DC. Listrik DC yang distandarisasi untuk disuntikkan adalah 48 volt, dengan arus sebesar 350 ampere, dengan maksimum daya 15,4 watt.

Setelah keempat kabel tadi dihubungkan dengan sumber listriknya, maka kini di dalam seutas kabel UTP Anda sudah terdapat dua buah jalur. Empat kabel pertama adalah jalur data dan empat kabel berikutnya adalah jalur listrik DC. Perangkat penyatu antara sinyal listrik dan sinyal data inilah yang disebut dengan PoE injector.

Di dalam perangkat jaringan penerimanya biasanya terdapat sebuah *receiver* yang akan berfungsi untuk memisahkan kembali antara sinyal listrik dan data. Sinyal listrik yang dikirimkan tadi diarahkan menuju ke modul DC/DC converter yang akan menerima sinyal listrik untuk kemudian digunakan mengaktifkan perangkat. Sedangkan jalur datanya tetap berada pada jalurnya semula yaitu menuju ke sistem pemrosesan data. Teknik ini hanya bisa bekerja dalam teknologi komunikasi Ethernet dan Fast Ethernet saja, sedangkan untuk teknologi Gigabit Ethernet yang memanfaatkan seluruh inti kabelnya, teknologi ini belum bisa digunakan.

Penyuntikan melalui kabel yang sama dengan jalur transmisi data.

Sistem PoE ini agak berbeda dengan yang telah dijelaskan di atas. Jika sistem di atas menggunakan kabel nganggur, teknik penyuntikan jenis ini tidak. Semua sinyal baik listrik maupun data disatukan dalam empat buah inti kabel. Hal ini dimungkinkan karena listrik DC yang disuntikkan ke dalam jalur data sebenarnya tidak akan mengganggu jalannya data karena data tersebut sebenarnya juga dalam bentuk sinyal-sinyal listrik DC. Hanya saja besar voltasenya berbeda dan lebih kecil dibandingkan listrik DC untuk mengaktifkan perangkat. Atas dasar inilah penggabungan bisa terjadi.

Setelah sinyal listrik DC dikirim secara kontiniu dan teratur, kemudian digabungkan dengan transmisi data dan dibawa dalam media yang sama, maka sinyal-sinyal DC ini sampai pada sisi penerimanya. Di sisi penerima, jalur sinyal listrik dan data dipisahkan dengan cara melakukan *center-tap* langsung di depan komponen TX dan RX dari perangkat penerima ini.

Ketika ada sinyal-sinyal listrik yang voltasenya sesuai dengan yang diinginkan oleh DC/DC Converter, maka sinyal listrik tadi diteruskan untuk menghidupkan perangkat. Jika tidak sesuai, maka sinyal tersebut diteruskan ke dalam sistem transmisi data untuk diolah lebih lanjut. Begitulah seterusnya sehingga sistem ini bukan hanya dapat digunakan untuk teknologi Ethernet dan Fast Ethernet saja, tetapi juga memungkinkan untuk teknologi Gigabit Ethernet.

Teknologi jenis ini akhirnya mencetuskan standardisasi baru bagi teknologi PoE dengan mewujudkan kemungkinan untuk memperbesar tenaga listrik yang dapat disuplai melalui media ini, berikut pernak-pernik monitoring, negosiasi, deteksi dan banyak lagi. Standardisasi ini diberi nama IEEE 802.3at.

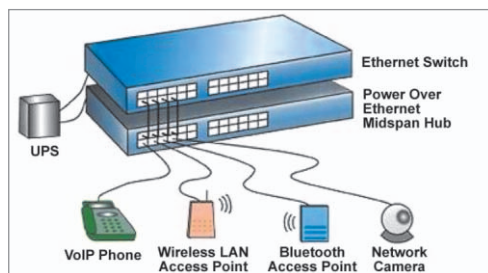
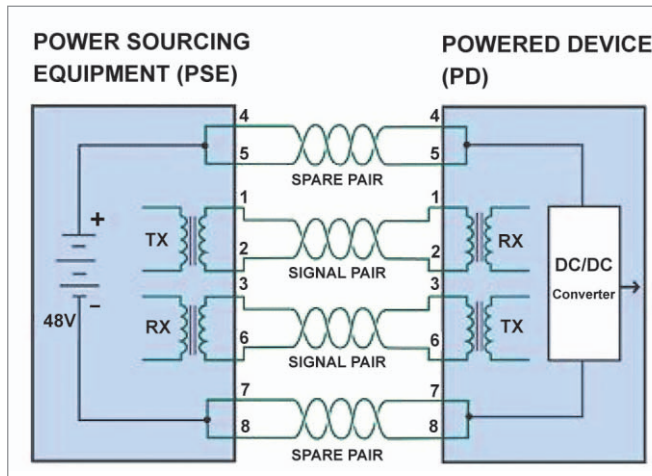
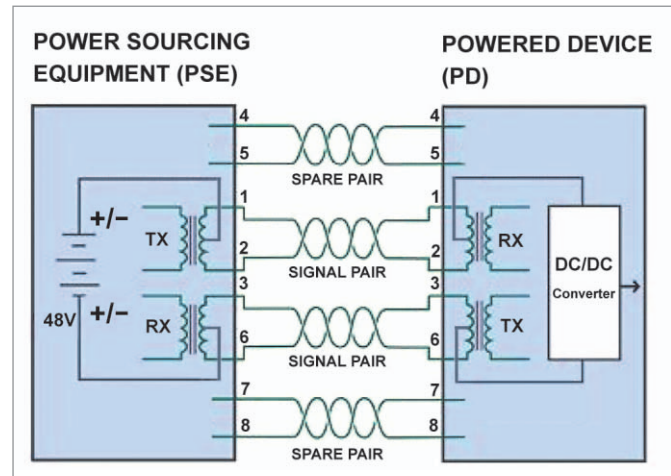
Jenis-jenis Perangkat PoE

Inline PoE

Inline PoE adalah jenis PoE yang dirancang untuk membagi satu media transportasi untuk digunakan bersama-sama membawa power atau tenaga listrik dan sinyal-sinyal data. Dengan demikian untuk mengaktifkan dan sekaligus menggunakan sebuah perangkat jaringan untuk berkomunikasi data, Anda hanya membutuhkan seutas kabel UTP saja. Tidak perlu adaptor atau kabel listrik lain untuk mengaktifkannya.

Untuk melakukan hal tersebut, perangkat PoE dilengkapi sebuah modul yang bernama PoE injector. PoE injector merupakan perangkat yang akan memadukan sumber-sumber sinyal komunikasi data seperti sinyal dari modem, switch, router, dan lain sebagainya, dengan sinyal-sinyal listrik yang akan digunakan untuk mengaktifkan perangkatnya.

PoE injector ini akan dihubungkan dengan kabel jalur data dan juga power outlet atau soket listrik yang umum digunakan yang akan berfungsi sebagai sumber listrik bagi perangkat di belakangnya. Jadi PoE injector ini bagaikan persimpangan jalan yang menggabungkan dua jalur menjadi satu.

Melihat fungsinya, biasanya PoE injector ini diletakkan di MDF atau ruangan distribusi data namun juga dekat dengan soket listrik atau sumber listrik lainnya. Kemudian sumber listrik tersebut dipanjangkan dengan menggunakan kabel UTP category 5 biasa.

Teknologi injeksi sinyal listrik DC pada kabel "nganggur".

Teknologi injeksi listrik DC dengan menggunakan jalur fisik yang sama dengan jalur data.

Teknologi PoE jenis ini adalah tipe yang paling umum digunakan. Banyak vendor perangkat jaringan yang menggunakan PoE jenis ini pada produknya. Tapi biasanya, produk yang dilengkapi fasilitas PoE adalah produk berskala *enterprise*, bukan pada produk-produk kelas rumahan. Jadi perangkat PoE biasanya akan Anda temukan di kantor-kantor kecil, perusahaan besar, pabrik-pabrik, dan banyak lagi.

Hub-based PoE

Alternatif lain untuk mengimplementasikan teknologi PoE untuk digunakan adalah dengan menginstal "power hub" di antara sumber sinyal dan akses point data Anda. Sebenarnya konsep dari hub-based PoE ini sama dengan sistem inline PoE, yaitu menjadi tempat bertemunya sinyal listrik dan data kemudian disatukan dalam satu jalur.

Hanya saja dengan sistem hub ini PoE dapat digunakan untuk melayani kebutuhan listrik dan transportasi data untuk lebih dari satu perangkat, seperti layaknya perangkat hub pada transportasi data. Dengan kata lain, dalam perangkat ini terdapat lebih dari satu PoE injector. Jadi jika Anda punya jalur-jalur data yang banyak, tinggal koneksikan saja pada terminasi data dari perangkat ini, kemudian port output-nya sudah mengubah jalur ini menjadi PoE.

Keuntungannya adalah Anda tidak perlu menyediakan banyak power outlet atau steker listrik untuk banyak perangkat. Cukup satu saja yang langsung terkoneksi pada PoE hub. Dengan demikian, Anda sudah menghemat biaya yang cukup banyak untuk menyediakan kabel listrik, soket listrik dan tempat untuk menjaga jalur kabel agar tetap rapi.

Hub-based PoE sangat cocok digunakan untuk keperluan jaringan berskala besar. Jika jaringan yang lama sudah terbentang dengan baik, hub PoE dapat dijadikan alternatif untuk membuat perluasan jaringan Anda ini, seperti memasang access point wireless. Biasanya PoE hub ini terdiri dari 12 port yang dapat mendistribusikan data dan sumber listrik. Keuntungan yang paling menonjol dari sistem ini adalah satu power untuk semuanya.

Integrated PoE

Cara yang paling nyaman untuk menggunakan teknologi PoE ini adalah dengan cara mengintegrasikan semua itu ke dalam switch. Jika PoE hub hanya bersifat sebagai pemanjang kabel saja bagi sinyal listrik dan data, integrated PoE yang terdapat pada switch ini akan berfungsi sebagai sumber distribusi utama bagi jaringan Anda. Anda tidak perlu membeli perangkat tambahan untuk membangun jaringan PoE ini.

Switch ini sendiri yang akan terkoneksi ke power outlet, switch ini juga yang akan menjadi terminasi data, switch ini juga yang bisa menjadi titik transit bagi data, dan switch ini pula yang bisa memperluas jaringan data Anda dengan menggunakan teknologi PoE. Jadi semua perangkat data dan PoE Anda dapat digabungkan di dalam switch ini untuk dapat berkomunikasi satu sama lain. Semuanya dapat dilakukan hanya dengan menggunakan jaringan kabel UTP category 5 saja sepeti layaknya switch-switch biasa.

Integrated PoE adalah solusi paling tepat untuk digunakan dalam membangun jaringan, terutama jaringan baru, yang sebagian besar perangkatnya adalah berteknologi PoE. Tetapi kendalanya adalah pada perusahaan-perusahaan besar biasanya sudah memiliki jaringan berskala besar yang masih menggunakan teknologi lama atau teknologi jaringan ethernet biasa. Dengan demikian pada umumnya teknologi integrated PoE hanya digunakan sebagai perluasan jaringan besar saja.

Tunggu Tanggal Mainnya

Teknologi ini memang sangat menjanjikan kemudahan. Bukan hanya kemudahan, Anda juga akan merasakan nilai ekonomis dari penggunaan perangkat ini. Anda tidak memerlukan biaya berlebih untuk membuat soket listrik yang banyak untuk perangkat Anda. Tidak perlu membuat sumber listrik yang banyak untuk menjalankan beberapa perangkat. Tidak perlu pemanjangan kabel listrik jika soket listrik tidak mencukupi, tidak perlu mengeluarkan banyak biaya untuk kabel listrik, dan banyak lagi keuntungannya.

Saat ini memang masih belum terlalu terdengar gaungnya di dalam kehidupan masyarakat. Tapi tunggu saja beberapa tahun lagi, ketika komunikasi data sudah sangat merasuk dalam kehidupan manusia. Pasti Anda akan jarang melihat bentangan kabel listrik di rumah, yang ada hanyalah jalur kabel UTP yang tipis dan kecil yang tidak terlalu memakan tempat dan juga biaya. ■

Lebih Lanjut

- **www.PowerOverEthernet.com**
- **http://standards.ieee.org/getieee802/download/802.3af-2003.pdf**
- **http://en.wikipedia.org/wiki/Power_over_Ethernet**

Gunung Sarjono

Menjadi Support yang Andal

Bagian 1 dari 2 Artikel

Pada deskripsi kerja terdapat sejumlah tanggung jawab, seperti instalasi, tes, pemeliharaan PC dan *hardware* jaringan, serta sistem *software*, tapi diperlukan suatu karakter untuk menjadi *support* yang andal bukan hanya kemampuan melakukan suatu tugas.

Coba lihat deskripsi kerja *support* dan Anda akan menemukan sejumlah keahlian standar dan tanggung jawab: instalasi, tes, pemeliharaan PC dan hardware jaringan serta sistem *software*; membuat dan memelihara penyimpanan komponen PC; membuat dokumentasi support, dan lainnya. Tapi, untuk menjadi support yang andal memerlukan lebih dari sekadar kemampuan melakukan tes diagnosis atau membuat *image workstation*. Keahlian dan pengetahuannya boleh saja sulit, tapi sikap dan ketangkasan tidak—mereka harus dipilih pada waktu support hendak dipekerjakan.

Menghormati Semua User, Anggota Tim, dan Atasan —meski Tidak Dibalas

Menunjukkan rasa hormat merupakan salah satu penghargaan atas nilai dan pengetahuan seseorang. Ini hal penting bagi seorang support. Jika user tidak percaya bahwa support tidak menangani masalahnya secara serius, mereka akan kurang mau berkomunikasi dan akan hilang kepercayaan terhadap teknologi, perlengkapan mereka, dan bagian TI secara keseluruhan. Sangat penting bagi seorang support untuk mempunyai kesabaran hingga bisa tetap menghormati user bahkan pada waktu menerima makian dari user. Meskipun dari perspektif support masalah user kelihatan sepele, yang paling penting adalah persepsi user atas masalah tersebut dan itulah yang perlu dijawab oleh support.

Displin Pribadi

Menjadi seorang yang disiplin mempengaruhi beberapa aspek tugas support, misalnya membuat dan melaksanakan jadwal, *deadline meeting*, memberi solusi kepada user pada atau sebelum tanggal/waktu yang dijanjikan, dan tetap pada tugasnya sampai selesai. Displin pribadi berhubungan dengan menghormati user; dengan membuat prioritas deadline, support menunjukkan rasa hormat terhadap waktu user. Support yang mempunyai disiplin pribadi lebih dapat diandalkan, tepat waktu dan bisa menerima lebih banyak tanggung jawab dibanding support yang kurang disiplin.

Bisa Menentukan Prioritas

Jika support diberi kontrol untuk mengatur waktunya, mereka harus bisa memberi prioritas tugasnya. Agar bisa memberikan prioritas secara efektif support harus tahu peran masing-masing karyawan dalam organisasi, pemahaman menyeluruh atas lingkungan kerja, dan pemahaman yang baik atas prioritas perusahaan. Jabatan dan/atau fungsi kerja dari karyawan yang meminta bantuan biasanya menjadi faktor utama dalam memberi prioritas tugas. Support harus sedapat mungkin mempelajari sistem kerja sehingga mereka bisa mendapatkan pengetahuan yang diperlukan untuk memberi prioritas secara efektif.

Dedikasi dan Komitmen untuk Memecahkan Masalah

Support harus mempunyai komitmen untuk melihat masalah sampai ke pemecahannya, yang hanya muncul pada waktu user puas bahwa masalah telah dipecahkan—dan pada waktu solusi tahan lama dan sesuai dengan kebijakan perusahaan.

Perhatikan contoh berikut: seorang user melaporkan bahwa ia tidak dapat menjalankan aplikasi yang baru diinstalasi. Sebagai langkah dalam mendiagnosis penyebab masalah, support menaikkan user tersebut dari akses terbatas ke akses penuh. User sekarang dapat menjalankan aplikasi, tetapi pekerjaan belum selesai karena kebijakan perusahaan mengharuskan user mempunyai akses terbatas. User berada dalam tekanan berat untuk mengirimkan data penting, sehingga support memutuskan untuk membiarkan dia untuk menyelesaikan pekerjaan dengan hak akses penuh. Jika support tidak berkomitmen untuk menyelesaikan pemecahan masalah, ia langsung menutup *work order* dan pergi, melanggar kebijakan sekuriti perusahaan. Support harus mau dan dapat mengikuti semua langkah dalam prosedur bahkan dalam situasi kritis.

Cara Kerja yang Terperinci

Memberi perhatian pada hal kecil adalah penting untuk menyelesaikan work order dengan baik. Meski memecahkan suatu masalah agar user puas adalah perlu, itu bukanlah kondisi yang cukup untuk menganggap bahwa work order sudah selesai. Misalnya, pada contoh sebelumnya, support masih harus menyelidiki penyebab masalah, perbaiki, tulis, dan mengembalikan user ke keadaannya yang biasa. Semakin lama support melakukan ini, makin banyak masalah yang muncul. Memberi perhatian pada hal yang kecil membantu dalam menciptakan lingkungan komputasi yang konsisten, aman, dan dapat diandalkan.

Kemampuan dan Mau Berkomunikasi

Dalam banyak organisasi, support adalah anggota bagian TI yang paling kelihatan dalam kontak sehari-hari dengan user. Dalam perannya sebagai perwakilan bagian TI dan sebagai mediator antara TI dan user, komunikasi yang efektif adalah sangat penting.

Support pada dasarnya harus menjadi *Babel Fish*, menerjemahkan antara bahasa teknis dan sehari-hari. Support harus belajar

mendengarkan user, melihat realitas masalah mereka, menerjemahkan deskripsi mereka ke dalam bahasa teknis, memperbaiki masalah, dan menjelaskan solusi dalam bahasa yang bisa dimengerti user.

Berbagi Pengetahuan dengan Anggota Tim, Atasan, dan User

Salah satu aspek khusus dari kemampuan komunikasi support adalah mau berbagi pengetahuan. Beberapa karyawan mencoba untuk mendapatkan pekerjaan dengan bermodalkan pengetahuan tertentu. Ini adalah hal yang salah, karena kebanyakan perusahaan sadar akan kelemahan yang timbul dan tidak ingin mempunyai karyawan semacam itu.

Mau berbagi pengetahuan adalah bagian penting dalam menjadi anggota tim. Kebanyakan support bekerja dalam tekanan berat dengan waktu yang sedikit untuk penelitian atau pelatihan, hingga mereka sering kali bergantung kepada anggota tim lain untuk meningkatkan pengetahuannya. Selain berbagi pengetahuan dengan yang lain, support harus mau mengedukasi user mereka. Melatih user supaya menggunakan aplikasi dan *peripheral* secara efektif dan mengajari mereka untuk melaporkan masalah komputer secara akurat akan membantu dalam mengurangi *downtime* user dan mempercepat pemecahan masalah.

Sikap Rendah Hati

Support harus menyadari, mereka tidak akan pernah tahu semua tentang suatu masalah—kuncinya adalah tahu di mana harus mencari informasi dan *resources* dan mau minta tolong pada waktu membutuhkan. Mereka harus siap untuk membaca manual dan menerima koreksi dari yang lain. Membutuhkan sikap rendah hati untuk membuka manual, menanyakan solusi kepada kolega, atau tekan [F1].

Kemampuan untuk Belajar dari Pengalaman dan dari Pelatihan Informal/Formal

Setelah bertahun-tahun sekolah dan mengikuti pelatihan teknis, terlalu naif jika support mau bersantai mengurangi kemauan untuk belajar. Dengan asumsi, sekarang mereka dipekerjakan pada profesi yang mereka pilih, mereka mempunyai semua pengetahuan yang diperlukan untuk melakukan pekerjaan. Ini mungkin benar pada lingkungan tertentu, tetapi jika support ingin berganti posisi dan/atau perusahaan, ia akan mendapatkan bahwa pengetahuannya sudah tertinggal dan penggunaannya terbatas. Karakteristik teknologi informasi yang berubah pesat, dan mereka yang ingin tetap produktif di dalamnya harus secara aktif mencari kesempatan untuk meningkatkan pengetahuannya, apakah melalui pelatihan formal dengan mengikuti kelas atau hanya membaca, berpartisipasi dalam forum, dan bertanya kepada rekan kerja.

Kemampuan untuk Berpikir Secara Logis dan Kreatif

Support harus bisa menggunakan metodologi yang konsisten dan logis dalam memecahkan

Kurang Koordinasi: Penyebab Tidak Bekerjanya Support

■ Tidak jarang bagian support diremehkan. Namun, perlu ditekankan bahwa mudah untuk menyalahkan orang lain pada waktu komputer tidak bekerja sebagaimana mestinya. Support jatuh pada beberapa hal, tetapi tidak hanya karena kurang usaha atau kemampuan. Ini berubah secara drastis sejak kemunculan Internet, dan beberapa masalah yang tidak bisa perbaiki. *Internet service provider* (ISP) mempengaruhi beratnya layanan support, dan margin profit membuat sebagian besar ISP membatasi staf *call center.*

Sejumlah masalah ini tidak mengenakkan buat bagian TI yang juga harus mendukung keseluruhan perusahaan.

Bagaimanapun Anda melihatnya, men-*support* sistem komputer pada waktu Internet terlibat tidak pernah menjadi pekerjaan yang mudah, dan menjadi semakin sulit—terutama pada waktu Anda menangani serangan virus, Trojan, dan segala macam *spyware*.

Support sangat mengandalkan kemampuan user untuk melakukan tugas, dan kita semua lebih dari sekadar familiar dengan sulitnya membantu *user* komputer yang tidak berpengalaman. Worm dan virus bisa tersebar luas karena kurangnya pemeliharaan sistem, biasanya sistem rumahan pada jaringan *broadband*.

Karena tidak bisa membantu user ini secara langsung, kita harus mengandalkan ISP mereka untuk membantu kita memperbaiki masalah karena mempengaruhi jaringan kita. Kita melihat *worm* dan virus datang dari jaringan lain sepanjang waktu, tetapi kita tidak berdaya untuk memperbaiki masalah tersebut.

Support jatuh lebih dalam dari yang kebanyakan orang tahu. Ini mengejutkan banyak orang pada waktu mereka tahu bahwa hampir tidak ada koordinasi antara ISP. ISP merupakan *front line* Internet, tetapi tidak ada cara pusat bagi support untuk berkomunikasi dengan menghubungi support yang lebih tingga pada waktu terjadi masalah. Puluhan ribu port discan setiap hari—kebanyakan karena worm—berasal dari perusahaan besar, perusahaan kecil, universitas, dan jaringan kabel serta DSL. Kadang-kadang kita bisa menghubungi orang-orang yang mengelola jaringan tersebut dan memberitahu mereka ada masalah, tetapi biasanya sulit.

Pindah *upstream* dan coba ISP mereka. Masih saja tidak membantu memperbaiki masalah karena banyak ISP mengotomatisasi sistem pelaporan masalah sehingga menolak e-mail yang bukan dari pelanggan mereka. Atau lebih buruk, pada waktu menelpon untuk melaporkan suatu masalah, kita menghadapi sikap yang arogan.

Keluhan utama mengenai support adalah para profesional TI tidak bekerja sama sebagai tim. Terlepas dari IS atau perusahaan mana Anda bekerja, jika Anda termasuk dalam support tingkat tinggi atau Anda adalah orang yang mempunyai otoritas dengan ISP besar, beritahu cara menghubungi Anda. Siapa tahu—mungkin jika sebagian dari kita mau bekerja sama sebagai tim dan merespon dengan cepat pada waktu masalah muncul, kita bisa mengurangi *bandwidth* yang terbuang pada Internet yang disebabkan oleh worm dan virus yang beraktivitas secara luas.

Seperti yang telah disebutkan, support semakin gagal lebih dari yang kebanyakan orang tahu. Ini mengejutkan banyak orang karena merekalah yang diandalkan orang untuk memperbaiki masalahnya. Jadi bagaimana jika bekerja sama dan memperlakukan seluruh Internet sebagai jaringan kita? Kita bisa mendapatkan lebih banyak dengan saling membantu daripada menyalahkan orang lain.

Hal-hal yang Dikeluhkan Support

Kita semua bekerja pada lingkungan yang berbeda, industri yang berbeda, dengan struktur bagian yang berbeda, instalasi yang berbeda, dan user yang berbeda. Tetapi sebagai *support*, kita semua bertujuan untuk membantu orang-orang dan komputer supaya hidup harmonis. Meskipun *hardware, software,* dan orang-orang berubah, gangguan cenderung sama.

User yang memaksakan diagnosis mereka bukannya menggambarkan gejalanya

Contoh klasik adalah seorang direktur yang terus-menerus memberitahukan bahwa koneksi *down* setiap kali ia tidak bisa browsing Internet atau masuk ke dalam SAP. Bukannya menggambarkan gejalanya, tetapi malah mengatakan "Koneksi down; tolong perbaiki." Perilaku semacam ini sudah pasti menjengkelkan. Bukan hanya mempersulit proses troubleshooting, tetapi juga sering kali sulit untuk membebaskan user ini dari kesalahpahamannya sehingga bisa saja mempunyai anggapan yang salah bahwa koneksi tidak andal.

User yang menunggui Anda sambil bertanya-tanya pada waktu troubleshooting—dan lebih parah, memberi saran

Meskipun suka berbagi pengetahuan dan mengedukasi user, kita tentu tidak ingin melakukannya pada waktu berusaha untuk mengetahui mengapa user tidak bisa mencetak. Ini sangat mengganggu terutama pada waktu menghadapi masalah yang ternyata tidak bisa dipecahkan, karena pada waktu user memberikan pertanyaan yang tidak bisa kita jawab, itu menunjukkan ketidakkompetenan kita.

User yang menyangkal tidak melakukan apapun yang bisa menyebabkan masalah

Ini merupakan fenomena "Apa? Zuma terinstalasi pada komputer saya? Saya betul-betul tidak tahu bagaimana itu bisa terjadi". Pada satu contoh, seorang user menelepon *help desk* untuk mengeluh bahwa aplikasi tidak tampil pada layar plasma. Setelah dilihat ternyata sebagian data dalam file konfigurasi telah diubah atau dihapus. Mereka secara tegas menyangkal telah melakukannya, tetapi pada akhirnya mengaku bahwa tadi tidak punya tugas yang perlu dikerjakan sehingga coba-coba "mempelajari" aplikasi.

Diperlakukan seperti user oleh support dari perusahaan lain

Kita mungkin tidak ingin menghadapi masalah yang ternyata harus menelepon support pabrikan. Kita akan mencoba, membaca manual, mencari di Yahoo! sebelum menelpon nomor support pabrikan atas masalah yang tidak bisa dipecahkan. Harga diri kita mungkin tidak bisa menerima untuk menjawab pertanyaan paling mendasar: Apakah Anda sudah mengecek bahwa kabel printer terhubung dan printer dinyalakan? *ARRRGGGH*. Tolong langsung hubungkan ke support yang paling tinggi karena dijamin kita telah mencoba semua yang akan disarankan paling sedikit tiga kali.

Bagian purchasing yang mengubah pengadaan

Kita mengerti dan menghargai bahwa sebagian peran dari bagian *purchasing* adalah untuk mendapatkan harga yang paling baik, tetapi kita tentu tidak suka pada waktu mereka mengganti suatu barang dengan apa yang mereka anggap ekivalen karena harganya lebih murah. Salah satu contoh adalah pada waktu meminta pengadaan memori untuk printer. Pada waktu datang, tidak disadari bahwa yang diberikan adalah merk yang berbeda dengan yang diminta. Tetap saja tidak bekerja karena pada waktu mengecek dokumentasi diketahui bahwa merk memory tersebut tidak bisa digunakan. Mereka melakukannya karena harga merk memory tersebut hanya sepertiga dari

Yang Perlu Dilakukan Sebelum Liburan

Anda berencana untuk berlibur jauh selama dua minggu. Meski Anda meninggalkan ponsel supaya liburan tidak terganggu dari laporan printer yang macet, *password* yang terlupa, dan lain sebagainya, bagaimana dengan yang ada di pikiran Anda? Agar Anda bisa berlibur dengan tenang, pastikan user tetap ditangani selagi Anda tidak ada. Berikut beberapa hal yang perlu dilakukan:

Password. Password apa yang hanya Anda yang tahu? Semua password penting harus ditulis dan disimpan pada tempat yang aman, misalnya brankas. Ini termasuk password Anda, meskipun mereka tidak penting. Liburan yang menyenangkan bisa menghilangkan hal-hal sepele dari pikiran Anda. Baru saja mengubah password dan tidak mengatakan kepada siapapun? Pastikan password yang baru diubah diberitahukan pada pihak yang berkepentingan.

Work order yang belum selesai. Apakah Anda mempunyai work order atau tanggung jawab lain yang belum diselesaikan? Pastikan Anda membereskan yang ditinggal dengan menyelesaikan work order, mendelegasikan ke pihak yang dapat diandalkan, atau meminta pengertian user untuk bersabar dan menunggu Anda kembali.

Tugas rutin. Identifikasi tugas yang yang menjadi tanggung jawab Anda. Apakah Anda mengganti tape back-up atau melakukan tugas malam? Dokumentasikan dan kemudian otomatisasi atau delegasikan semua tugas itu. Jika Anda harus mendelegasikan tugas rutin, buat *reminder* beberapa menit sebelum tugas dilakukan.

Rencana kerja. Ini mungkin sepele, tetapi setelah kembali dari liburan bisa saja Anda lupa. Jadi daripada berasumsi bahwa rekan kerja Anda akan mengingatnya, buat daftar dan delegasikan.

Kiriman yang ditunggu. Memesan sesuatu akhir-akhir ini? Jika Anda menantikan suatu kiriman, terutama jika itu sangat ditunggu user, pastikan orang lain tahu apa yang ditunggu dan kapan, serta apa yang dilakukan pada waktu barang tiba. Minta pada orang yang menerima untuk memeriksanya secara akurat. Tentu mengecewakan jika setelah kembali dari liburan bukannya menerima barang yang diharapkan, tapi malah barang yang salah.

merk yang diminta. Ternyata yang terjadi malah pemborosan hanya karena ini menghemat biaya.

Junk mail internal
Kita ingin mengurangi jumlah *junk mail* yang dikirim dalam organisasi, tetapi tampaknya hanya sedikit yang bisa dilakukan untuk menghilangkan lelucon, foto, dan film yang di-*share* secara internal. Kebijakan untuk mencegah atau bahkan melarang mail pribadi penggunaannya terbatas kecuali jika mail diperiksa secara manual. Jika hanya menggunakan sistem e-mail perusahaan saja untuk mengirim mail prbadi bukanlah masalah besar, tetapi pada waktu orang-orang mulai secara bebas menggunakan "Everyone" atau membuat folder untuk "Resep", "Basket", kita cenderung sedikit terganggu.

User yang menganggap sebagian dari pekerjaan kita adalah menghabiskan istirahat makan siang kita untuk memberitahu mereka bagaimana cara memperbaiki komputer di rumah mereka
Pada waktu suatu wawancara pekerjaan, calon atasan memberitahu bahwa ia hanya memperkerjakan orang yang "makan, tidur, dan memikirkan komputer 24/7". Bukan tidak ada salahnya terobsesi dengan komputer; hanya saja kita bukan orang seperti itu. Jika seperti itu, kita mungkin menerima saja pada waktu makan siang diganggu dengan "Setiap kali saya mengakses Internet, pesan ini muncul dan kemudian mouse diam. Apa yang terjadi?" Kita lebih dari sekedar senang membantu orang. Kita hanya tidak suka diminta melakukan suatu pekerjaan pada waktu istirahat.

User yang mengeluh tidaik bisa menggunakan suatu aplikasi baru, karena mereka "tidak punya waktu: untuk mengikuti training atau membaca dokumentasi yang telah Anda persiapakan dengan seksama
Situasi ini sangat menjengkelkan karena biasanya, user benar-benar tidak punya waktu untuk mengikuti training atau membaca dokumentasi—jadi akan tidak adil jika saya menimpakan kekesalan pada user tersebut. Ini merupakan tanda dari suatu masalah yang jauh lebih besar yang mengharapkan terlalu banyak dari karyawan yang terlalu sedikit. Bukannya merasa jengkel terhadap orang-orang semacam ini, tetapi kita harus bersimpati terhadap mereka kerena mereka biasanya orang-orang yang paling banyak pekerjaannya dan paling tertekan dalam organisasi.

Dipanggil ke kantor user untuk mengatasi masalah penting, tetapi diminta menunggu
Ini tambah menjengkelkan pada waktu orang yang dimaksud sedang melakukan telepon pribadi untuk membicarakan rencana akhir pekan. Kita tidak tahu berapa lama harus menunggu. Jika langsung pergi terkesan kasar, tetapi jika kita menunggu selama selang waktu tertentu, pergi dan datang lagi beberapa menit kemudian hanya menambah total waktu yang terbuang. Untungnya, pada user yang paling keras kepala, memperlakukan user seperti *sales* kartu kredit dengan meninggalkan mereka biasanya akan mendapatkan respon positif.

Posisi bagian TI dalam organisasi
Kebanyakan bagian mengetahui posisinya di dalam organisasi, tetapi tak seorangpun cukup tahu apa hubungannya dengan TI. Sering kali bagian TI dimasukkan ke dalam bagian lain, yang kemudian tidak bisa mengontrol resources TI dengan benar. Contoh lain, masing-masing bagian atau divisi mempunyai TI sendiri bisa saja mempunyai hubungan yang kurang jelas dengan TI perusahaan.

masalah. Ini berarti bahwa meski pada waktu dihadapkan dengan situasi baru, support kemungkinan besar akan dapat memecahkan masalah, atau paling tidak membatasi masalah. Untuk mem-back-up pemikiran logis mereka, support juga harus bisa membuat lompatan kreatif pada waktu penggunaan logika tidak menghasilkan pemecahan yang memuaskan.

Kemampuan Menggunakan Pengetahuan pada Situasi Baru

Kemampuan ini bersama dengan pemikiran yang logis dan kreatif, membentuk *troubleshooter* yang andal. Beberapa support baik sekali dalam mengikuti prosedur yang ditentukan pada situasi yang familiar, tapi betul-betul terhalang pada waktu dihadapkan dengan situasi asing. Kemampuan mengadaptasi suatu pengetahuan pada situasi baru sangat penting; tidak mungkin untuk melatih support untuk menghadapi setiap situasi. Troubleshooting memerlukan kemampuan untuk mengaplikasikan pengetahuan.

Minat Pribadi akan Teknologi

Kita mungkin pernah meninggalkan suatu wawancara kerja pada waktu diberitahu bahwa mereka mencari kandidat yang "hidup, bernafas, tidur, berjalan, dan berbicara tentang teknologi". Biasanya orang seperti ini sering kali menjadi support yang jelek, karena kurang dalam hubungan antarperseorangan. Meskipun begitu, jika seorang support tidak mempunyai minat pribadi terhadap teknologi dan hanya karena berhubungan dengan pekerjaan, maka membuat support tetap *up-to-date* atau mendapatkan kepuasan kerja akan menjadi perjuangan panjang.

Mempunyai support yang tertarik dan senang akan teknologi baru menjadi penting terutama pada waktu pembaruan, di mana support mempengaruhi sikap user terhadap perubahan dalam lingkungannya. Pembaruan bisa membuat user tertekan karena mereka sekarang harus belajar produk baru untuk melakukan pekerjaannya. Mempunyai support yang tertarik dan senang akan produk baru akan mendorong dan meyakinkan user.

Mempunyai seorang support yang tertarik dan senang terhadap teknologi baru menjadi penting terutama pada waktu pembaruan, di mana support mempengaruhi sikap user terhadap perubahan dalam lingkungannya. Pembaruan bisa membuat user tertekan karena mereka sekarang harus belajar produk baru untuk melakukan pekerjaan mereka. Mempunyai support yang tertarik dan senang terhadap produk baru akan mendorong dan meyakinkan user. ■

Lebih Lanjut

- **http://en.wikipedia.org/wiki/Babelfish**